PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-202719
(43)Date of publication of application : 19.07.2002

(51)Int.Cl. G09C 1/00
G06F 12/14

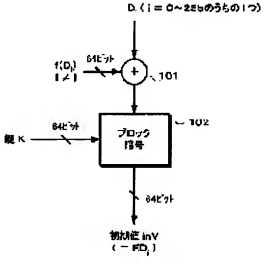
(21)Application number : 2001-066850
(22)Date of filing : 09.03.2001

(71)Applicant : SONY CORP
(72)Inventor : SAKO YOICHIRO
FURUKAWA SHUNSUKE
INOGUCHI TATSUYA
KIHARA TAKASHI

(30)Priority
Priority number : 2000337307 Priority date : 06.11.2000 Priority country : JP

(54) DEVICE AND METHOD FOR ENCIPHERING, DEVICE AND METHOD FOR DECIPHERING, AND STORAGE MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a device and a method for enciphering which enable carrying out of a chain of enciphering without necessitating data or random numbers in a special area for an initial value and have high confidentiality nature, and to provide a device and method for deciphering and a storage medium.
SOLUTION: When data on contents are enciphered and recorded, the data on contents are divided into blocks and the blocks are chained in a chain-like status and enciphered. The initial value at this time is generated from the contents data itself in its sector. In the case of an MPEG stream, the initial value is generated from unique information on a header. Thus, it is not necessary to generate initial value by random numbers, etc., and loss of a data area will not occur. Since the contents data change at random, the confidentiality nature is high. Moreover, the circuit scale can be kept small, because a random number generator and the like is not necessary.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－202719
（P2002－202719A）
(43)公開日　平成14年７月19日(2002.7.19)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード（参考）
Ｇ０９Ｃ　1/00	６１０	Ｇ０９Ｃ　1/00	６１０Ｂ　５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｂ　５Ｊ１０４

審査請求　未請求　請求項の数56　ＯＬ　（全 26 頁）

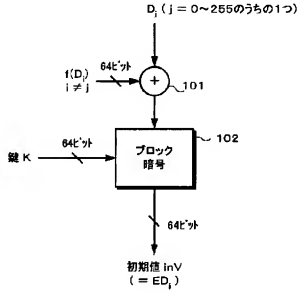
(21)出願番号　特願2001－66850(P2001－66850)
(22)出願日　平成13年３月９日(2001.3.9)
(31)優先権主張番号　特願2000－337307(P2000－337307)
(32)優先日　平成12年11月６日(2000.11.6)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　佐古　曜一郎
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　古川　俊介
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100082762
弁理士　杉浦　正知

最終頁に続く

(54)【発明の名称】　暗号化装置及び方法、復号装置及び方法、並びに記憶媒体

(57)【要約】
【課題】　連鎖的な暗号化を行う場合に、初期値のための特別な領域のデータや乱数が不要であると共に、秘匿性が高くなるようにする。また、データ領域が有効に利用できるようにする。
【解決手段】　コンテンツのデータを暗号化して記録する際に、コンテンツのデータがブロック化され、鎖状に連鎖して暗号化される。このときの初期値は、そのセクタのコンテンツデータそのものから生成される。ＭＰＥＧストリームの場合には、ヘッダのユニークな情報から生成される。このため、初期値を乱数等で発生させる必要がなく、データ領域のロスがない。また、コンテンツデータはランダムに変化しているため、秘匿性が高い。更に、乱数発生器等を用意する必要がなく、回路規模が増大しない。



1

【特許請求の範囲】

【請求項１】　コンテンツデータの第１の部分のデータに応じて初期値を生成する生成手段と、

上記生成された初期値に応じて上記コンテンツデータの第２の部分のデータを暗号化し、暗号化データを出力すると共に、当該出力される暗号化データに応じて、上記コンテンツデータの第１及び第２の部分のデータとは異なる部分のデータを連鎖的に暗号化する暗号手段とを備えるようにした暗号化装置。

【請求項２】　更に、上記コンテンツデータを複数ビットからなるブロック単位に分割する分割手段を備え、

上記生成手段は、上記分割されたブロック単位で、当該ブロック内の第１の部分のデータに応じて初期値を生成するようにした請求項１に記載の暗号化装置。

【請求項３】　上記暗号手段は、上記分割されたブロック単位で、ブロック暗号化方式により暗号化を行うようにした請求項２に記載の暗号化装置。

【請求項４】　上記初期値を暗号化するようにした請求項１に記載の暗号化装置。

【請求項５】　上記コンテンツデータの第１の部分のデータを変更可能とした請求項１に記載の暗号化装置。

【請求項６】　コンテンツデータの第１の部分のデータに応じて初期値を生成し、

上記生成された初期値に応じて上記コンテンツデータの第２の部分のデータを暗号化し、暗号化データを出力すると共に、当該出力される暗号化データに応じて、上記コンテンツデータの第１及び第２の部分のデータとは異なる部分のデータを連鎖的に暗号化するようにした暗号化方法。

【請求項７】　更に、上記コンテンツデータを複数ビットからなるブロック単位に分割し、

上記分割されたブロック単位で、当該ブロック内の第１の部分のデータに応じて初期値を生成するようにした請求項６に記載の暗号化方法。

【請求項８】　上記分割されたブロック単位で、ブロック暗号化方式により暗号化を行うようにした請求項７に記載の暗号化方法。

【請求項９】　上記初期値を暗号化するようにした請求項６に記載の暗号化方法。

【請求項１０】　上記コンテンツデータの第１の部分のデータを変更可能とした請求項６に記載の暗号化方法。

【請求項１１】　暗号化されたコンテンツデータの第１の部分のデータを初期値とし、上記暗号化されたコンテンツデータの第２の部分データと上記初期値から上記第２の部分を復号化し、当該復号データを出力すると共に、上記第１及び第２の部分のデータとは異なる部分の暗号化データと、その前の暗号化データとから連鎖的に上記第１及び第２の部分のデータとは異なる部分を復号化する復号手段と、

上記暗号化されたコンテンツデータの第１の部分のデータから上記第１の部分のデータを生成する生成手段とを備えるようにした復号装置。

2

【請求項１２】　更に、上記コンテンツデータは、複数ビットからなるブロック単位で暗号化されており、

上記復号手段は、上記ブロック単位で、ブロック暗号化方式により復号化を行うようにした請求項１１に記載の復号装置。

【請求項１３】　上記生成手段は、上記ブロック単位で、上記暗号化されたコンテンツデータの第１の部分のデータから上記第１の部分のデータを生成するようにした請求項１２に記載の復号装置。

【請求項１４】　上記初期値は暗号化されており、上記第１の部分のデータを上記初期値を復号して生成するようにした請求項１１に記載の暗号化装置。

【請求項１５】　暗号化されたコンテンツデータの第１の部分のデータを初期値とし、上記暗号化されたコンテンツデータの第２の部分データと上記初期値から上記第２の部分を復号化し、当該復号データを出力すると共に、上記第１及び第２の部分のデータとは異なる部分の暗号化データと、その前の暗号化データとから連鎖的に上記第１及び第２の部分のデータとは異なる部分を復号化し、

上記暗号化されたコンテンツデータの第１の部分のデータから上記第１の部分のデータを生成するようにした復号方法。

【請求項１６】　更に、上記コンテンツデータは、複数ビットからなるブロック単位で暗号化されており、

上記ブロック単位で、ブロック暗号化方式により復号化を行うようにした請求項１５に記載の復号方法。

【請求項１７】　上記ブロック単位で、上記暗号化されたコンテンツデータの第１の部分のデータから上記第１の部分のデータを生成するようにした請求項１６に記載の復号方法。

【請求項１８】　上記初期値は暗号化されており、上記第１の部分のデータを上記初期値を復号して生成するようにした請求項１５に記載の復号方法。

【請求項１９】　コンテンツデータの第１の部分のデータに応じて初期値を生成し、

上記生成された初期値に応じて上記コンテンツデータの第２の部分のデータを暗号化し、暗号化データを出力すると共に、当該出力される暗号化データに応じて、上記コンテンツデータの第１及び第２の部分のデータとは異なる部分のデータを連鎖的に暗号化して、上記コンテンツのデータを記憶するようにした記憶媒体。

【請求項２０】　コンテンツデータのストリームの所定の部分のデータに応じて初期値を生成する生成手段と、

上記生成された初期値に応じて上記コンテンツデータを暗号化し、暗号化データを出力すると共に、当該出力される暗号化データに応じて、上記コンテンツデータとは異なる部分のデータを連鎖的に暗号化する暗号手段とを

備えるようにした暗号化装置。

【請求項２１】　更に、上記コンテンツデータを複数ビットからなるブロック単位に分割する分割手段を備え、上記暗号手段は、上記分割されたブロック単位で、ブロック暗号化方式により暗号化を行うようにした請求項２０に記載の暗号化装置。

【請求項２２】　上記ストリーム中のヘッダの部分に含まれるデータに応じて初期値を生成するようにした請求項２０に記載の暗号化装置。

【請求項２３】　上記ストリーム中のヘッダの部分に含まれる時間情報に応じて初期値を生成するようにした請求項２０に記載の暗号化装置。

【請求項２４】　上記ストリーム中のヘッダの部分に含まれるコンテンツ毎にユニークな情報に応じて初期値を生成するようにした請求項２０に記載の暗号化装置。

【請求項２５】　上記ストリーム中のヘッダの部分に含まれる時間情報と、上記ストリーム中のヘッダの部分に含まれるコンテンツ毎にユニークな情報とに応じて初期値を生成するようにした請求項２０に記載の暗号化装置。

【請求項２６】　上記初期値を暗号化するようにした請求項２０に記載の暗号化装置。

【請求項２７】　上記ストリームは、ＭＰＥＧストリームである請求項２０に記載の暗号化装置。

【請求項２８】　上記ヘッダは、パックヘッダ、パケットヘッダ、又はファイルヘッダである請求項２７に記載の暗号化装置。

【請求項２９】　コンテンツデータのストリームの所定の部分のデータに応じて初期値を生成し、
上記生成された初期値に応じて上記コンテンツデータを暗号化し、暗号化データを出力すると共に、当該出力される暗号化データに応じて、上記コンテンツデータとは異なる部分のデータを連鎖的に暗号化するようにした暗号化方法。

【請求項３０】　更に、上記コンテンツデータを複数ビットからなるブロック単位に分割し、
上記分割されたブロック単位で、ブロック暗号化方式により暗号化を行うようにした請求項２９に記載の暗号化方法。

【請求項３１】　上記ストリーム中のヘッダの部分に含まれるデータに応じて初期値を生成するようにした請求項２９に記載の暗号化方法。

【請求項３２】　上記ストリーム中のヘッダの部分に含まれる時間情報に応じて初期値を生成するようにした請求項２９に記載の暗号化方法。

【請求項３３】　上記ストリーム中のヘッダの部分に含まれるコンテンツ毎にユニークな情報に応じて初期値を生成するようにした請求項２９に記載の暗号化方法。

【請求項３４】　上記ストリーム中のヘッダの部分に含まれる時間情報と、上記ストリーム中のヘッダの部分に含まれるコンテンツ毎にユニークな情報とに応じて初期値を生成するようにした請求項２９に記載の暗号化方法。

【請求項３５】　上記初期値を暗号化するようにした請求項２９に記載の暗号化方法。

【請求項３６】　上記ストリームは、ＭＰＥＧストリームである請求項２９に記載の暗号化方法。

【請求項３７】　上記ヘッダは、パックヘッダ、パケットヘッダ、又はファイルヘッダである請求項３６に記載の暗号化方法。

【請求項３８】　コンテンツデータのストリームの所定の部分のデータに応じて初期値を生成する生成手段と、暗号化されたコンテンツデータと上記初期値から上記コンテンツデータを復号化し、当該復号データを出力すると共に、暗号化データと、その前の暗号化データとから連鎖的にコンテンツデータを復号化する復号手段とを備えるようにした復号装置。

【請求項３９】　更に、上記コンテンツデータは、複数ビットからなるブロック単位で暗号化されており、
上記復号手段は、上記ブロック単位で、ブロック暗号化方式により復号化を行うようにした請求項３８に記載の復号装置。

【請求項４０】　上記生成手段は、上記ストリーム中のヘッダの部分に含まれるデータに応じて初期値を生成するようにした請求項３８に記載の復号装置。

【請求項４１】　上記生成手段は、上記ストリーム中のヘッダの部分に含まれる時間情報に応じて初期値を生成するようにした請求項３８に記載の復号装置。

【請求項４２】　上記生成手段は、上記ストリーム中のヘッダの部分に含まれるコンテンツ毎にユニークな情報に応じて初期値を生成するようにした請求項３８に記載の復号装置。

【請求項４３】　上記生成手段は、上記ストリーム中のヘッダの部分に含まれる時間情報と、上記ストリーム中のヘッダの部分に含まれるコンテンツ毎にユニークな情報とに応じて初期値を生成するようにした請求項３８に記載の復号装置。

【請求項４４】　上記生成手段は、暗号化されている上記初期値を復号化するようにした請求項３８に記載の復号装置。

【請求項４５】　上記ストリームは、ＭＰＥＧストリームである請求項３８に記載の復号装置。

【請求項４６】　上記ヘッダは、パックヘッダ、パケットヘッダ、又はファイルヘッダである請求項４５に記載の復号装置。

【請求項４７】　コンテンツデータのストリームの所定の部分のデータに応じて初期値を生成し、
暗号化されたコンテンツデータと上記初期値から上記コンテンツデータを復号化し、当該復号データを出力すると共に、暗号化データと、その前の暗号化データとから

連鎖的にコンテンツデータを復号化するようにした復号方法。

【請求項４８】　更に、上記コンテンツデータは、複数ビットからなるブロック単位で暗号化されており、

上記復号手段は、上記ブロック単位で、ブロック暗号化方式により復号化を行うようにした請求項４７に記載の復号装置。

【請求項４９】　上記生成手段は、上記ストリーム中のヘッダの部分に含まれるデータに応じて初期値を生成するようにした請求項４７に記載の復号装置。

【請求項５０】　上記生成手段は、上記ストリーム中のヘッダの部分に含まれる時間情報に応じて初期値を生成するようにした請求項４７に記載の復号装置。

【請求項５１】　上記生成手段は、上記ストリーム中のヘッダの部分に含まれるコンテンツ毎にユニークな情報に応じて初期値を生成するようにした請求項４７に記載の復号装置。

【請求項５２】　上記生成手段は、上記ストリーム中のヘッダの部分に含まれる時間情報と、上記ストリーム中のヘッダの部分に含まれるコンテンツ毎にユニークな情報とに応じて初期値を生成するようにした請求項４７に記載の復号装置。

【請求項５３】　上記生成手段は、暗号化されている上記初期値を復号化するようにした請求項４７に記載の復号装置。

【請求項５４】　上記ストリームは、ＭＰＥＧストリームである請求項４７に記載の復号装置。

【請求項５５】　上記ヘッダは、パックヘッダ、パケットヘッダ、又はファイルヘッダである請求項５４に記載の復号装置。

【請求項５６】　コンテンツデータのストリームの所定の部分のデータに応じて初期値を生成し、

上記生成された初期値に応じて上記コンテンツデータを暗号化し、暗号化データを出力すると共に、当該出力される暗号化データに応じて、上記コンテンツデータとは異なる部分のデータを連鎖的に暗号化して、上記コンテンツのデータを記憶するようにした記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、例えばＣＤ（Compact Disc）２のような光ディスクに、オーディオデータ等のコンテンツのデータを記録／再生する際に、コンテンツのデータの保護を図るためにデータを暗号化して記録するのに用いて好適な暗号化装置及び方法、復号装置及び方法、並びに記憶媒体に関する。

【０００２】

【従来の技術】近年、大容量の記録媒体として光ディスクの開発が進められてきている。例えば音楽情報が記録されたＣＤ(Compact Disc)、コンピュータ用のデータが記録されるＣＤ－ＲＯＭ、映像情報を取り扱うＤＶＤ(Digital Versatile Disc またはDigital Video Disc) 等が知られている。

【０００３】ここに挙げた光ディスクは、読み出し専用のディスクである。最近では、ＣＤ－Ｒ(CD-Recordable)ディスク 、ＣＤ－ＲＷ(CD-Rewritable)ディスク等のように、データの追記や、書き換えが可能な光ディスクが実用化されている。さらに、ＣＤと同様な形状で記録容量を高めた倍密度ＣＤや、通常のＣＤプレーヤとパーソナルコンピュータとの双方との親和性が高められるＣＤ２等、様々な光ディスクの開発が進められている。

【０００４】このような光ディスクの普及に伴って、光ディスクに記録されたコンテンツのデータが不正に複製されて使用されたり、複製されたものが不正に販売されたりして、著作権者に不利益を与えることが危惧されている。そこで、光ディスクにオーディオデータやビデオデータのようなコンテンツデータを記録する際に、著作権者の権利を保護することを目的として、コンテンツデータに対して暗号化処理を施こすことが行われている。

【０００５】このように、光ディスクにコンテンツのデータを記録する際に用いる暗号化方式としては、ＤＥＳ（Data Encryption Standard）やtripple ＤＥＳ等のブロック暗号が使われてきている。ＤＥＳは代表的な共通鍵暗号であり、６４ビット（８バイト）のデータを初期転置（スクランブル）を行い、３２ビットずつ分けたデータを、５６ビットの１個の暗号鍵から生成された１６個の鍵で次々と非線形処理を行い、再び転置を行って、暗号化するものである。

【０００６】ところが、ＤＥＳのようなブロック暗号は、ブロックの長さが比較的短いため、類似のブロックが頻繁に現れる可能性があり、暗号強度に問題がある。

【０００７】そこで、暗号強度を上げるために、ＣＢＣ（Ciphering Block Chaining ） 方式を用いることが考えられている。ＣＢＣ方式は、ブロック単位で暗号化したデータを連鎖させていくことで暗号強度を上げていくものである。

【０００８】すなわち、ＣＢＣ方式では、暗号化を行う際には、今回の入力ブロックデータと、その１つ前のブロックデータを暗号化したデータとのＥＸ－ＯＲがとられ、暗号化される。復号化を行う際には、暗号化ブロックデータが復号化され、その前の暗号化ブロックデータとのＥＸ－ＯＲがとられて、元のブロックデータが復号される。このように、ＣＢＣ方式では、前のブロックデータと連鎖させながら暗号化されるため、暗号強度を上げることができる。

【０００９】

【発明が解決しようとする課題】このように、光ディスクにコンテンツのデータを記録する際に、ＣＢＣ方式で暗号化を行うと、暗号強度が上げられ、より、強力に、著作権の保護を図ることができる。ところが、ＣＢＣ方式では、前のブロックデータと連鎖させながら暗号化し

ていくため、暗号化を行う際の最初のブロックでは、直前の暗号化ブロックがないため、初期値を用意する必要がある。このようにＣＢＣ方式で暗号化を行う際の初期値としては、固定値を使うことが最も簡単である。ところが、ＣＢＣ方式の暗号化を行う際の初期値として固定値を用いたのでは、秘匿性に問題があり、高い暗号強度が維持できない。また、初期値として固定値を用意するためには、この初期値となる固定値をどこかにストアしておく必要が生じる。

【００１０】そこで、暗号化のブロックには含まれていない他の領域のデータから初期値を作ることが考えられる。例えば、エラー訂正のためのＥＣＣ（Error CorrectingCode ）や媒体情報が含まれている。これらのデータは、著作権を有するようなデータそのものではないので、保護する必要はなく、通常、暗号化のブロックには含められない。そこで、ＥＣＣや媒体情報のような、他の領域のデータから初期値を作ることが考えられる。

【００１１】つまり、図２５は、ＥＣＣや媒体情報のような他の領域のデータから、ＣＢＣ方式で暗号化を行う際の初期値を作るようにした例である。図２５に示すように、入力ブロックデータＤｉ を０～２５５までの２５６個のブロックデータとし、１ブロックは８バイト（６４ビット）とする。

【００１２】最初に、初期値ｉＮＶとして、他の領域からのデータが入力され、ＥＸ－ＯＲゲート５０１で、入力ブロックデータＤ０ と初期値ｉＮＶとのＥＸ－ＯＲがとられ、これがブロック暗号化回路５０２で鍵情報Ｋにより暗号化されて、暗号化ブロックデータＥＤ０ が生成される。

【００１３】次に、ＥＸ－ＯＲゲート５０１で、入力ブロックデータＤ１ と、その前の暗号化ブロックデータＥＤ０ とのＥＸ－ＯＲがとられ、これがブロック暗号化回路１０２で鍵情報Ｋにより暗号化されて、暗号化ブロックデータＥＤＩ が生成される。

【００１４】以下、入力ブロックデータＤｉ と、その前の暗号化ブロックデータＥＤｉ-１ とのＥＸ－ＯＲがとられ、これがブロック暗号化回路５０２で鍵情報Ｋにより暗号化されて、暗号化ブロックデータＥＤｉが生成される。

【００１５】このように、初期値ｉＮＶをブロックのデータ以外、例えば、ＥＣＣや媒体情報から作るようにすれば、初期値が固定値とならないため、秘匿性が上がる。

【００１６】ところが、このように、初期値ｉＮＶをブロックのデータ以外、例えば、ＥＣＣや媒体情報から作るようにすると、コンテンツデータ以外のデータが暗号化のために必ず必要になる。このため、コンテンツデータのみを暗号化してデータ伝送することができなくなり、コンテンツのデータを伝送する際には、必ず、ＥＣＣや媒体情報を一緒に送る必要が生じてくる。

【００１７】また、ＣＢＣ方式で暗号化を行う際の初期値を発生するための他の方法として、初期値を乱数により発生させることが考えられる。

【００１８】つまり、図２６に示すように、最初に、乱数により発生された値が初期値としてブロックデータＤ０ に入れられる。

【００１９】この初期値の入ったブロックデータＤ０ は、ブロック暗号化回路５１２で鍵情報Ｋにより暗号化されて、暗号化ブロックデータＥＤ１ が生成される。

【００２０】次に、ＥＸ－ＯＲゲート５１１で、入力ブロックデータＤ１ と、その前の暗号化ブロックデータＥＤ０ とのＥＸ－ＯＲがとられ、これがブロック暗号化回路５１２で鍵情報Ｋにより暗号化されて、暗号化ブロックデータＥＤ１ が生成される。

【００２１】以下、入力ブロックデータＤｉ と、その前の暗号化ブロックデータＥＤｉ-１ とのＥＸ－ＯＲがとられ、これがブロック暗号化回路５１２で鍵情報Ｋにより暗号化されて、暗号化ブロックデータＥＤｉが生成される。

【００２２】しかしながら、このように、乱数により初期値を発生させると、ブロックデータＤ０ には乱数により発生された初期値が入ることになり、ブロックデータＤ０には、コンテンツデータが入れられなくなる。したがって、１セクタの０～２５５までの２５６ブロック（２０４８バイト）のうちの２０４０バイトにしかコンテンツデータを入れることができなくなり、データ領域が有効に利用できないという問題が生じてくる。

【００２３】また、初期値を乱数により発生させるようにするためには、乱数発生回路が必要になる。秘匿性を高めるためには、乱数としてランダムな符号を発生できるものが必要であり、このような乱数発生回路を設けると、回路規模が増大するという問題が生じてくる。

【００２４】したがって、この発明の目的は、連鎖的な暗号化を行う場合に、初期値のための特別な領域のデータや乱数が不要であり、しかも、秘匿性が高い暗号化装置及び方法、復号装置及び方法、並びに記憶媒体を提供することにある。

【００２５】この発明の他の目的は、連鎖的な暗号化を行う場合に、データ領域が有効に利用できる暗号化装置及び方法、復号装置及び方法、並びに記憶媒体を提供することにある。

【００２６】

【課題を解決するための手段】請求項１の発明は、コンテンツデータの第１の部分のデータに応じて初期値を生成する生成手段と、生成された初期値に応じてコンテンツデータの第２の部分のデータを暗号化し、暗号化データを出力すると共に、当該出力される暗号化データに応じて、コンテンツデータの第１及び第２の部分のデータとは異なる部分のデータを連鎖的に暗号化する暗号手段とを備えるようにした暗号化装置である。

【００２７】請求項６の発明は、コンテンツデータの第１の部分のデータに応じて初期値を生成し、生成された初期値に応じてコンテンツデータの第２の部分のデータを暗号化し、暗号化データを出力すると共に、当該出力される暗号化データに応じて、コンテンツデータの第１及び第２の部分のデータとは異なる部分のデータを連鎖的に暗号化するようにした暗号化方法である。

【００２８】請求項１１の発明は、暗号化されたコンテンツデータの第１の部分のデータを初期値とし、暗号化されたコンテンツデータの第２の部分データと初期値から第２の部分を復号化し、当該復号データを出力すると共に、第１及び第２の部分のデータとは異なる部分の暗号化データと、その前の暗号化データとから連鎖的に第１及び第２の部分のデータとは異なる部分を復号化する復号手段と、暗号化されたコンテンツデータの第１の部分のデータから第１の部分のデータを生成する生成手段とを備えるようにした復号装置である。

【００２９】請求項１５の発明は、暗号化されたコンテンツデータの第１の部分のデータを初期値とし、暗号化されたコンテンツデータの第２の部分データと初期値から第２の部分を復号化し、当該復号データを出力すると共に、第１及び第２の部分のデータとは異なる部分の暗号化データと、その前の暗号化データとから連鎖的に第１及び第２の部分のデータとは異なる部分を復号化し、暗号化されたコンテンツデータの第１の部分のデータから第１の部分のデータを生成するようにした復号方法である。

【００３０】請求項１９の発明は、コンテンツデータの第１の部分のデータに応じて初期値を生成し、生成された初期値に応じてコンテンツデータの第２の部分のデータを暗号化し、暗号化データを出力すると共に、当該出力される暗号化データに応じて、コンテンツデータの第１及び第２の部分のデータとは異なる部分のデータを連鎖的に暗号化して、コンテンツのデータを記憶するようにした記憶媒体である。

【００３１】請求項２０の発明は、コンテンツデータのストリームの所定の部分のデータに応じて初期値を生成する生成手段と、生成された初期値に応じてコンテンツデータを暗号化し、暗号化データを出力すると共に、当該出力される暗号化データに応じて、コンテンツデータとは異なる部分のデータを連鎖的に暗号化する暗号手段とを備えるようにした暗号化装置である。

【００３２】請求項２９の発明は、コンテンツデータのストリームの所定の部分のデータに応じて初期値を生成し、生成された初期値に応じてコンテンツデータを暗号化し、暗号化データを出力すると共に、当該出力される暗号化データに応じて、コンテンツデータとは異なる部分のデータを連鎖的に暗号化するようにした暗号化方法である。

【００３３】請求項３８の発明は、コンテンツデータのストリームの所定の部分のデータに応じて初期値を生成する生成手段と、暗号化されたコンテンツデータと初期値からコンテンツデータを復号化し、当該復号データを出力すると共に、暗号化データと、その前の暗号化データとから連鎖的にコンテンツデータを復号化する復号手段とを備えるようにした復号装置である。

【００３４】請求項４７の発明は、コンテンツデータのストリームの所定の部分のデータに応じて初期値を生成し、暗号化されたコンテンツデータと初期値からコンテンツデータを復号化し、当該復号データを出力すると共に、暗号化データと、その前の暗号化データとから連鎖的にコンテンツデータを復号化するようにした復号方法である。

【００３５】請求項５６の発明は、コンテンツデータのストリームの所定の部分のデータに応じて初期値を生成し、生成された初期値に応じてコンテンツデータを暗号化し、暗号化データを出力すると共に、当該出力される暗号化データに応じて、コンテンツデータとは異なる部分のデータを連鎖的に暗号化して、コンテンツのデータを記憶するようにした記憶媒体である。

【００３６】コンテンツのデータがブロック化され、鎖状に連鎖して暗号化される。そして、このときの初期値を、そのセクタのコンテンツデータそのものから生成している。このため、初期値を乱数等で発生する必要がなく、データ領域のロスがない。また、コンテンツデータはランダムに変化しているため、秘匿性が高い。更に、乱数発生器等を容易する必要がなく、回路規模が増大しない。

【００３７】また、コンテンツデータから生成される初期値自体が他のコンテンツデータで暗号化される。更に、初期値として使うコンテンツデータを自由に選ぶことができる。これにより、秘匿性が向上される。

【００３８】さらに、ＭＰＥＧストリームを記録する場合には、ヘッダに含まれるユニークな情報を使って、初期値を生成している。ヘッダの情報はユニークであり、ＳＣＲやＰＴＳのような時間情報は、時間と共に変化するため、秘匿性が高い。また、ＭＰＥＧストリームのヘッダの情報を使って暗号化の初期値を形成しているので、ＭＰＥＧストリームを保ったまま、伝送することができる。さらに、乱数発生器等を容易する必要がなく、回路規模が増大しない。

【００３９】

【発明の実施の形態】以下、この発明の実施の形態について図面を参照して説明する。この発明は、例えば、ＣＤ（Compact Disc）２にコンテンツデータを記録／再生する際に、データの保護を図るために、コンテンツのデータを暗号化するのに用いて好適である。

【００４０】図１は、この発明が適用できるＣＤ２の外観の構成を示すものである。ＣＤ２は、通常のＣＤと同様に、例えば直径１２０ｍｍの光ディスクである。ただ

し、所謂シングルCDのように、直径８０mmとしても良い。

【００４１】CD２は、既存のCDプレーヤと、パーソナルコンピュータとの双方との親和性を考慮して開発されている。このようなCD２は、図１に示すように、その中心にセンターホールが設けられ、内周側に領域ＡＲ１が設けられ、さらにその外周に、領域ＡＲ２が設けられる。内周側の領域ＡＲ１と、外周側の領域ＡＲ２との間には、ミラー部Ｍ１が設けられ、このミラー部Ｍ１により、内周側の領域ＡＲ１と外周側の領域ＡＲ２とが区切られている。内周側の領域ＡＲ１の最内周には、リードイン領域ＬＩＮ１が設けられ、その最外周には、リードアウト領域ＬＯＵＴ１が設けられる。外周側の領域ＡＲ２の最内周には、リードイン領域ＬＩＮ２が設けられ、その最外周には、リードアウト領域ＬＯＵＴ２が設けられる。

【００４２】内周側の領域ＡＲ１は、既存のCDプレーヤとの親和性が図られた領域である。この領域ＡＲ１には、通常のCDプレーヤでも再生できるように、例えば、オーディオデータが通常のCD－DA（CD Digital Audio）と同様なフォーマットで記録されている。また、この内周側の領域ＡＲ１は、通常のCD－DAと同様に扱えるように、通常、コンテンツのデータに対する暗号化は行われない。勿論、著作権の保護を図るために、この内周側の領域ＡＲ１に記録するデータを暗号化する場合も考えられる。また、この内周側の領域ＡＲ１に、ビデオデータや、コンピュータプログラムデータ等、オーディオデータ以外のデータを記録するようにしても良い。また、この内周側の領域ＡＲ１に、コンテンツのデータを圧縮して記録するようにしても良い

【００４３】これに対して、外周側の領域ＡＲ２は、パーソナルコンピュータとの親和性を図るようにした領域である。この領域ＡＲ２には、倍密度でデータが記録できる。この領域ＡＲ２には、例えば、オーディオデータが圧縮されて記録される。圧縮方式としては、例えばＭＰ３（Mpeg-I Audio Layer-３）方式が用いられており、また、パーソナルコンピュータとの親和性が図れるように、ファイル化されている。

【００４４】ＭＰ３は、ＭＰＥＧ１で規定されている３つのレイヤの圧縮方式の１つであり、各帯域の出力をＭＤＣＴ（Modified Cosine Transform）で周波数軸に分割し、量子化した後、ハフマン符号化するようにしたものである。オーディオデータをＭＰ３方式で圧縮することで、記録容量を拡大できると共に、パーソナルコンピュータと同様のファイルシステムでデータを扱うことができる。このため、外周側の領域ＡＲ２にＭＰ３方式でファイル化されて記録されているコンテンツのデータを、パーソナルコンピュータのハードディスクに移動させて、パーソナルコンピュータに音楽サーバを構築したり、フラッシュメモリが装着される携帯型のＭＰ３再生プレーヤに移動させて、外で音楽再生を楽しんだりすることが容易になる。

【００４５】このように、外周側の領域ＡＲ２に記録されているコンテンツのデータは、パーソナルコンピュータとの親和性が図られ、取り扱いが容易である。ところが、この外周側の領域ＡＲ２に記録されているコンテンツのデータは、外部に持ち出されることが多くなるため、著作権の保護が守られなくなる可能性が高い。このため、外周側の領域ＡＲ２に記録されるコンテンツのデータには、コピーや再生を制限するために、暗号化処理が施されるとともに、この外周側の領域ＡＲ２には、例えば、コピー禁止／許可、コピーの世代管理、コピーの僅数制限、再生禁止／許可、再生回数の制限、再生時間の制限等を管理するための著作権管理情報が記録される。

【００４６】なお、ここでは、領域ＡＲ２に記録するデータをＭＰ３でファイル化しているが、勿論、領域ＡＲ２に記録されるコンテンツのデータは、ＭＰ３のファイルに限られるものではない。オーディオデータの圧縮方式としては、ＭＰ３の他に、ＭＰＥＧ２－ＡＡＣ（Advanced Audio Coding）、ＡＴＲＡＣ３等が知られている。また、オーディオデータに限らず、ビデオデータや静止画データ、テキストデータ、コンピュータプログラム等、様々なデータを領域ＡＲ２に記録することが可能である。また、領域ＡＲ２に記録するコンテンツのデータであっても、暗号化する必要がなければ、暗号化せずに記録しても良い、

【００４７】このように、CD２は、内周側の領域ＡＲ１を使って、通常のCDと同様にCDプレーヤで再生することができ、外周側の領域ＡＲ２を使うことで、パーソナルコンピュータや携帯型のプレーヤと連携させながら、データ扱うことができる。

【００４８】この発明は、このようなCD２において、特に、外周側の領域ＡＲ２に、コンテンツのデータを暗号化して記録／再生するのに用いて好適である。

【００４９】図２は、この発明が適用された記録装置の一例である。図２において、入力端子１にコンテンツデータが供給される。コンテンツデータは、例えば、オーディオデータである。オーディオデータとしては、ＰＣＭデータでも良いし、ＭＰ３等のストリームであっても良い。また、オーディオデータの他、動画データ、静止画データ、ゲームのプログラムデータ、ウェブページのデータ、テキスト等、種々のものをコンテンツデータとして記録することが考えられる。この入力端子１からのコンテンツデータは、暗号化回路４に供給される。

【００５０】また、入力端子２には鍵情報Ｋが供給される。入力端子２からの鍵情報Ｋが暗号化回路４に供給される。

【００５１】暗号化回路４は、入力端子１からのコンテンツデータを、入力端子２からの鍵情報Ｋを用いて暗号

化するものである。暗号化方式としては、ブロック暗号が用いられる。ブロック暗号は、例えば、８バイトずつを単位として暗号化を行っており、暗号化回路４はブロック化回路を備えている。この例では、ブロック単位で暗号化したデータを連鎖させていくことで、暗号化強度を上げるようにしている。このように、ブロック単位で暗号化したデータを連鎖させていくようなものは、ＣＢＣ（Ciphering Block Chaining ）方式として知られている。

【００５２】暗号化回路４の出力がエラー訂正符号化回路５に供給される。エラー訂正符号化回路５で、暗号化回路４で暗号化されたコンテンツデータに対して、エラー訂正符号が付加される。

【００５３】エラー訂正符号化回路５の出力は、変調回路６に供給される。変調回路６で、記録データが所定の変調方式で変調される。変調回路６の出力が記録回路７に供給される。

【００５４】記録回路７の出力が光学ピックアップ８に供給される。記録回路７は、システムコントローラ１３により制御される。光学ピックアップ８により、光ディスク１０に、データが記録される。光ディスク１０は、例えば、ＣＤ２の光ディスクである。

【００５５】光学ピックアップ８は、光ディスク１０の半径方向に移動可能とされている。また、図示していないが、光学ピックアップ８からのレーザー光を光ディスク１０のトラックに沿って照射するためのトラッキングサーボ回路や、光学ピックアップ８からのレーザー光のスポットを光ディスク１０上に合焦させるためのフォーカスサーボ回路、光ディスク１０の回転を制御するスピンドルサーボ回路等、各種のサーボ回路が設けられている。

【００５６】また、入力端子２からの鍵情報Ｋがミックス回路９に供給される。入力端子３に著作権管理情報Ｒが供給され、この著作権管理情報Ｒが書き換え回路１１を介して、ミックス回路９供給される。ミックス回路９の出力が記録回路１２を介して光学ピックアップ８に供給される。光学ピックアップ８により、記録回路１２により、光ディスク１０に鍵情報Ｋや著作権管理情報Ｒが記録される。

【００５７】著作権管理情報Ｒは、例えば、コピー禁止／許可、コピーの世代管理、コピーの個数制限、再生禁止／許可、再生回数の制限、再生時間の制限等を管理するための情報である。コピーの世代管理やコピーの個数制限、再生回数の制限や再生時間の制限を行う場合には、コピーや再生が行われる毎に、著作権管理情報Ｒを書き換える必要がある。この著作権管理情報Ｒの書き換えは、書き換え回路１１により行われる。

【００５８】また、鍵情報Ｋや著作権管理情報Ｒの記録場所については、光ディスク１０のリードインやリードアウト領域に記録したり、トラックの半径方向にウォブルデータとして記録したりすることが考えられる。

【００５９】図３は、再生系の構成を示すものである。図３において、光ディスク２０の記録信号は、光学ピックアップ２２で再生される。光ディスク２０は、図２における光ディスク１０と対応しており、光ディスク２０としては、例えば、ＣＤ２が用いられる。光学ピックアップ２２の出力が再生アンプ２３を介して、復調回路２４に供給される。光学ピックアップ２２の動きは、システムコントローラ２９の制御の基に、アクセス制御回路３０により制御される。アクセス制御回路３０は、光学ピックアップの送り機構、光学ピックアップ２２からのレーザー光を光ディスク２０のトラックに沿って照射するためのトラッキングサーボ回路や、光学ピックアップ２２からのレーザー光のスポットを光ディスク２０上に合焦させるためのフォーカスサーボ回路等のサーボ回路からなる。

【００６０】復調回路２４の出力がエラー訂正回路２５に供給される。エラー訂正回路２５で、エラー訂正処理がなされる。エラー訂正回路２５の出力が暗号解読回路２６に供給されると共に、鍵管理情報読出回路２７に供給される。鍵管理情報読出回路２７の出力が暗号解読回路２６に供給される。

【００６１】暗号解読回路２６は、鍵管理情報読出回路２７で読み出された鍵情報Ｋを使って、再生データの暗号解読の処理を行うものである。前述したように、この例では、暗号化方式として、ＣＢＣ方式が使われている。暗号解読回路２６は、このようなＣＢＣ方式の暗号の解読処理を行うものである。

【００６２】暗号解読回路２６の出力が再生回路２８に供給される。再生回路２８の出力が出力端子３１から出力される。また、鍵管理情報読出回路２７で読み出された著作権管理情報Ｒにより、コピーや再生が制限される。

【００６３】上述のように、この例では、暗号化方式として、ＣＢＣ方式が使われている。すなわち、記録系においては、暗号化回路４で、入力されたコンテンツデータに対して、ＣＢＣ方式により、暗号化処理が行われる。そして、再生系においては、暗号解読回路２６により、再生されたコンテンツデータに対して、暗号解読処理が行われる。

【００６４】なお、ブロック暗号は、ＤＥＳやＡＥＳ、ＦＥＡＬ、ＭＩＳＴＹ等、何を用いても良い。

【００６５】ＣＢＣ方式では、ブロック単位で暗号化したデータを連鎖させることで、暗号の強度が上げられる。この例では、図４に示すように、２０４８バイトが１セクタとされ、このセクタを単位として、光ディスク１０、２０へのデータの記録／再生が行われる。

【００６６】つまり、ＣＤでは、９８フレームからなるサブコードブロックが１セクタとされている。この１セクタの領域の大きさは２３５２バイトであり、そのう

ち、２０４８バイトがデータ領域となっている。

【００６７】例えば、ＤＥＳ方式で暗号化する場合には、６４ビットを１ブロックとして処理され、５６ビットの鍵が用いられる。このため、図５に示すように、１セクタは、８バイト（６４ビット）単位で、２５６のブロックに分割される。

【００６８】そして、各セクタ内において、前ブロックと連鎖させながら、ＣＢＣ方式により、暗号化処理が行われる。

【００６９】すなわち、ＣＢＣ方式では、今回のブロックデータと、その１つ前のブロックデータを暗号化したデータとのＥＸ－ＯＲがとられ、これが暗号化される。１つのセクタ内でＣＢＣ方式により暗号化処理が終了したら、次のセクタで、また、同様に、ＣＢＣ方式により暗号化処理が行われる。

【００７０】このように、この例では、ＣＢＣ方式を用いることにより、暗号の強度が上げられる。そして、各セクタでＣＢＣ方式で暗号化が行われている。このため、エラーの発生等によりデータの再生が不可能になったような場合でも、その影響がそのセクタ内で完結し、他のセクタにおよぶことがなくなる。

【００７１】そして、この発明の実施の形態では、初期値として、同一セクタ内のブロックのデータが利用される。このように、同一のセクタ内のブロックのデータを初期値として使うことで、データ領域のロスがなくなる。また、音楽データや画像データのようなコンテンツデータの場合には、それ自体の値がランダムに変化している。このため、コンテンツのデータを利用すると、初期値の秘匿性も高い。

【００７２】初期値として同一セクタ内のブロックのデータを利用する場合、そのデータそのものでは、秘匿性が十分でない。そこで、同一のセクタ内のブロックのデータを暗号化したものを初期値として利用することが考えられる。更に、この例では、同一セクタ内の１つのブロックデータと、そのセクタ内のそれ以外のブロックデータとのＥＸ－ＯＲをとり、これを暗号化したものを初期値としている。

【００７３】つまり、図６及び図７を使って、暗号化処理について説明する。図６は、初期値を生成するときのプロセスを示し、図７は、連鎖的にブロック暗号を行うときのプロセスを示すものである。

【００７４】暗号化処理を行う場合には、先ず、図６に示すようにして、初期値が生成される。

【００７５】すなわち、図６に示すように、Ｄ０～Ｄ２５５までの１セクタ内のブロックデータのうちの１つＤｊがＥＸ－ＯＲゲート１０１に送られる。また、同一のセクタ内のブロックデータＤｊを除くブロックデータＤｉの関数ｆ（Ｄｉ）がＥＸ－ＯＲゲート１０１に送られる。

【００７６】ＥＸ－ＯＲゲート１０１で、ブロックデータＤｊと、ブロックデータＤｊ以外のブロックデータＤｉの関数ｆ（Ｄｉ）とのＥＸ－ＯＲが求められる。

【００７７】なお、ブロックデータＤｊと、ブロックデータＤｊ以外のすべてのブロックデータＤｉの関数ｆ（Ｄｉ）とのＥＸ－ＯＲは、ブロックデータＤｊと、ブロックデータＤｊ以外のすべてのブロックデータＤｉの関数ｆ（Ｄｉ）とのＥＸ－ＯＲでも良いし、ブロックデータＤｊと、ブロックデータＤｊ以外の１つのブロックデータＤｉの関数ｆ（Ｄｉ）とのＥＸ－ＯＲでも良いし、ブロックデータＤｉの数をいくつにしても良い。また、関数ｆ（Ｄｉ）も、何を用いても良い。

【００７８】このＥＸ－ＯＲゲート１０１の出力は、ブロック暗号化回路１０２に送られる。ブロック暗号化回路１０２で、ＥＸ－ＯＲゲート１０１の出力が鍵情報Ｋにより暗号化される。これにより、初期値ｉｎＶが求められる。また、この値は、ブロックデータＤｊを暗号化したデータＥＤｊとしても用いられる。

【００７９】このようにして、初期値が求められたら、図７に示すように、この初期値を使って、今回のブロックデータと、その１つ前のブロックデータを暗号化したデータとのＥＸ－ＯＲがとられ、これが暗号化される。そして、ブロックデータＤｊのときには、初期値としても使われているデータＥＤｊが暗号化したブロックデータとして使われる。

【００８０】つまり、初期値として使った入力ブロックデータＤｊが（ｊ＝１～２５４）の何れかであるときには、以下のようにして暗号化が行われる。

【００８１】先ず、ＥＸ－ＯＲゲート１１１で、入力ブロックデータＤ０と、図６で求められた初期値ｉｎＶとのＥＸ－ＯＲがとられ、このＥＸ－ＯＲゲート１１１の出力がブロック暗号化回路１１２に供給される。

【００８２】ブロック暗号化回路１１２で、ＥＸ－ＯＲゲート１１１の出力と鍵情報Ｋとから、暗号化ブロックデータＥＤ０が求められる。

【００８３】次に、ＥＸ－ＯＲゲート１１１で、入力ブロックデータＤ１と、暗号化ブロックデータＥＤ０とのＥＸ－ＯＲがとられ、このＥＸ－ＯＲゲート１１１の出力がブロック暗号化回路１１２に供給され、ブロック暗号化回路１１２で、ＥＸ－ＯＲゲート１１１の出力と鍵情報Ｋとから、暗号化ブロックデータＥＤ１が求められる。

【００８４】以下、同様にして、入力データＤ２、Ｄ３、…から、暗号化ブロックデータＥＤ２、ＥＤ３、…が求められる。

【００８５】入力ブロックデータＤ２、Ｄ３、…を暗号化していき、入力ブロックデータがＤｊになったら、図６で求められた初期値ｉｎＶが暗号化ブロックデータＥＤｊとして出力される。

【００８６】そして、再び、ＥＸ－ＯＲゲート１１１で、入力ブロックデータＤｉと、暗号化ブロックデータ

ＥＤi-1 とのＥＸ－ＯＲがとられ、このＥＸ－ＯＲゲート１１１の出力がブロック暗号化回路１１２に供給され、ブロック暗号化回路１１２で、ＥＸ－ＯＲゲート１１１の出力と鍵情報Ｋとから、暗号化ブロックデータＥＤｉが求められる。

【００８７】入力データＤ255 が暗号化されて暗号化ブロックデータＥＤ255 が出力されるまで、同様の処理が繰り返される。

【００８８】初期値として使った入力ブロックデータＤｊが最初のブロックデータ（ｊ＝０）のときには、以下のようにして暗号化が行われる。

【００８９】先ず、図６で求められた初期値ｉｎＶが暗号化ブロックデータＥＤ０として出力される。

【００９０】それから、図７に示すＥＸ－ＯＲゲート１１１で、入力ブロックデータＤ１と、暗号化ブロックデータＥＤ０（初期値ｉｎＶと等しい）とのＥＸ－ＯＲゲートがとられ、このＥＸ－ＯＲゲート１１１の出力がブロック暗号化回路１１２に供給され、ブロック暗号化回路１１２で、ＥＸ－ＯＲゲート１１１の出力と鍵情報Ｋとから、暗号化ブロックデータＥＤ１が求められる。

【００９１】以下、入力データＤ255 が暗号化されて暗号化ブロックデータＥＤ255 が出力されるまで、同様の処理が繰り返され、入力データＤ２、Ｄ３、…から、暗号化ブロックデータＥＤ２、ＥＤ３、…が求められる。

【００９２】初期値として使った入力ブロックデータＤｊが最後のブロックデータ（ｊ＝２５５）のときには、以下のようにして暗号化が行われる。

【００９３】先ず、図７に示すＥＸ－ＯＲゲート１１１で、入力ブロックデータＤ０と、図６で求められた初期値ｉｎＶとのＥＸ－ＯＲがとられ、このＥＸ－ＯＲゲート１１１の出力がブロック暗号化回路１１２に供給される。

【００９４】ブロック暗号化回路１１２で、ＥＸ－ＯＲゲート１１１の出力と鍵情報Ｋとから、暗号化ブロックデータＥＤ０が求められる。

【００９５】次に、ＥＸ－ＯＲゲート１１１で、入力ブロックデータＤ１と、暗号化ブロックデータＥＤ０とのＥＸ－ＯＲがとられ、このＥＸ－ＯＲゲート１１１の出力がブロック暗号化回路１１２に供給され、ブロック暗号化回路１１２で、ＥＸ－ＯＲゲート１１１の出力と鍵情報Ｋとから、暗号化ブロックデータＥＤ１が求められる。

【００９６】以下、同様にして、入力データＤ２、Ｄ３、…から、暗号化ブロックデータＥＤ２、ＥＤ３、…が求められる。入力データＤ254 の暗号化ブロックデータＥＤ254 が求められるまで、同様の処理が繰り返される。

【００９７】最後のブロックデータＤ255 になったら、図６で求められた初期値ｉｎＶが暗号化ブロックデータＥＤ255 として出力される。

【００９８】次に、図８及び図９を使って、復号化処理について説明する。図８は、連鎖的にブロック暗号を行うときのプロセスを示すものであり、図９は、初期値を暗号化したブロックデータを復号するときのプロセスを示すものである。

【００９９】初期値として使った入力ブロックデータＤｊが（ｊ＝１～２５４）の何れかであるときには、以下のようにして復号化が行われる。

【０１００】先ず、図８に示すように、暗号化ブロックデータＥＤ０と、鍵情報Ｋとがブロック暗号復号回路１２１に送られ、ブロック暗号復号回路１２１で、暗号の復号処理が行われる。

【０１０１】ブロック暗号復号回路１２１の出力がＥＸ－ＯＲゲート１２２に送られる。また、ＥＸ－ＯＲゲート１２２には、初期値ｉｎＶが送られる。この初期値ｉｎＶは、暗号化ブロックデータＥＤｊである。

【０１０２】ＥＸ－ＯＲゲート１２２で、ブロック暗号復号回路１２１の出力と、暗号化ブロックデータＥＤｊとのＥＸ－ＯＲがとられて、ブロックデータＤ０が復号される。

【０１０３】次に、暗号化ブロックデータＥＤ１と、鍵情報Ｋとがブロック暗号復号回路１２１に送られる。ブロック暗号復号回路１２１で暗号が復号される。ブロック暗号復号回路１２１の出力がＥＸ－ＯＲゲート１２２に送られる。

【０１０４】また、ＥＸ－ＯＲゲート１２２には、その前の暗号化ブロックデータＥＤ０とが送られる。

【０１０５】ＥＸ－ＯＲゲート１２２で、ブロック暗号復号回路１２１の出力と、その前の暗号化ブロックデータＥＤ０とのＥＸ－ＯＲがとられて、ブロックデータＤ１が復号される。

【０１０６】以下、同様にして、暗号化ブロックデータＥＤ１、ＥＤ２、…から、ブロックデータＤ１、Ｄ２、…が復号されていく。

【０１０７】このように、ブロックデータＤ２、Ｄ３、…を復号化していく間に、復号するブロックデータが初期値に相当する暗号化ブロックデータＥＤｊになったら、図９に示すように、暗号化ブロックデータＥＤｊと、鍵情報ＫとがブロックＢ暗号復号回路１３１に送られ、ブロック暗号復号回路１３１で暗号の復号処理が行われる。

【０１０８】ブロック暗号復号回路１３１の出力がＥＸ－ＯＲゲート１３２に送られる。また、ＥＸ－ＯＲゲート１３２には、ブロックデータＤｊ以外のデータとの間の関数ｆ（Ｄｉ）が送られる。

【０１０９】ＥＸ－ＯＲゲート１３２で、ブロック暗号復号回路１３１の出力と、ブロックデータＤｊ以外のデータとの間の関数ｆ（Ｄｉ）とのＥＸ－ＯＲがとられて、ブロックデータＤｊが復号される。

【０１１０】ブロックデータＤｊが復号されたら、図８

に戻り、暗号化ブロックデータＥＤｉ と、鍵情報Ｋとがブロック暗号復号回路１２１に送られる。ブロック暗号復号回路１２１で暗号が復号される。ブロック暗号復号回路１２１の出力がＥＸ－ＯＲゲート１２２に送られる。また、ＥＸ－ＯＲゲート１２２には、その前の暗号化ブロックデータＥＤｉ-1 が送られる。ＥＸ－ＯＲゲート１２２で、ブロック暗号復号回路１２１の出力と、その前の暗号化ブロックデータＥＤｉ-1 とのＥＸ－ＯＲがとられて、ブロックデータＤｉ が復号される。

【０１１１】以下、暗号化ブロックデータＥＤ255 が復号されるまで、同様な処理が繰り返される。

【０１１２】初期値として使った入力ブロックデータＤｊ が最初のブロックデータ（ｊ＝０）のときには、以下のようにして復号化が行われる。

【０１１３】先ず、図９に示すように、暗号化ブロックデータＥＤ０ と、鍵情報Ｋとがブロック暗号復号回路１３１に送られ、ブロック暗号復号回路１３１で暗号の復号処理が行われる。

【０１１４】ブロック暗号復号回路１３１の出力がＥＸ－ＯＲゲート１３２に送られる。また、ＥＸ－ＯＲゲート１３２には、ブロックデータＤ０ 以外のデータとの間の関数ｆ（Ｄｉ ）が送られる。

【０１１５】ＥＸ－ＯＲゲート１３２で、ブロック暗号復号回路１３１の出力と、ブロックデータＤｊ 以外のデータとの関数ｆ（Ｄｉ ）とのＥＸ－ＯＲがとられて、ブロックデータＤ０ が復号される。

【０１１６】ブロックデータＤ０ が復号されたら、図８に示すように、暗号化ブロックデータＥＤ１ と、鍵情報Ｋとがブロック暗号復号回路１２１に送られ、ブロック暗号復号回路１２１で、暗号の復号処理が行われる。

【０１１７】ブロック暗号復号回路１２１の出力がＥＸ－ＯＲゲート１２２に送られる。また、ＥＸ－ＯＲゲート１２２には、初期値ｉｎＶが送られる。初期値ｉｎＶは、暗号化ブロックデータＥＤ０ である。

【０１１８】ＥＸ－ＯＲゲート１２２で、ブロック暗号復号回路１２１の出力と、暗号化ブロックデータＥＤ０ とのＥＸ－ＯＲがとられて、ブロックデータＤ１ が復号される。

【０１１９】次に、暗号化ブロックデータＥＤ２ と、鍵情報Ｋとがブロック暗号復号回路１２１に送られる。ブロック暗号復号回路１２１で暗号解読処理が行われる。

【０１２０】ブロック暗号復号回路１２１の出力がＥＸ－ＯＲゲート１２２に送られる。また、ＥＸ－ＯＲゲート１２２には、その前の暗号化ブロックデータＥＤ１ が送られる。

【０１２１】ＥＸ－ＯＲゲート１２２で、ブロック暗号復号回路１２１の出力と、その前の暗号化ブロックデータＥＤ１ とのＥＸ－ＯＲがとられて、ブロックデータＤ２ が復号される。

【０１２２】以下、暗号化ブロックデータＥＤ255 が復号されるまで、同様な処理が繰り返される。

【０１２３】初期値として使った入力ブロックデータＤｊ が最後のブロックデータ（ｊ＝２５５）のときには、以下のようにして復号化が行われる。

【０１２４】先ず、図８に示すように、暗号化ブロックデータＥＤ０ と、鍵情報Ｋとがブロック暗号復号回路１２１に送られ、ブロック暗号復号回路１２１で、暗号の復号処理が行われる。

【０１２５】ブロック暗号復号回路１２１の出力がＥＸ－ＯＲゲート１２２に送られる。また、ＥＸ－ＯＲゲート１２２には、初期値ｉｎＶが送られる。この初期値ｉｎＶは、暗号化ブロックデータＥＤ255 である。

【０１２６】ＥＸ－ＯＲゲート１２２で、ブロック暗号復号回路１２１の出力と、暗号化ブロックデータＥＤ255 とのＥＸ－ＯＲがとられて、ブロックデータＤ０ が復号される。

【０１２７】次に、暗号化ブロックデータＥＤ１ と、鍵情報Ｋとがブロック暗号復号回路１２１に送られる。ブロック暗号復号回路１２１で暗号が復号される。ブロック暗号復号回路１２１の出力がＥＸ－ＯＲゲート１２２に送られる。

【０１２８】また、ＥＸ－ＯＲゲート１２２には、その前の暗号化ブロックデータＥＤ０ が送られる。

【０１２９】ＥＸ－ＯＲゲート１２２で、ブロック暗号復号回路１２１の出力と、その前の暗号化ブロックデータＥＤ０ とのＥＸ－ＯＲがとられて、ブロックデータＤ１ が復号される。

【０１３０】以下、同様にして、暗号化ブロックデータＥＤ２ 、ＥＤ３ 、…から、ブロックデータＤ２ 、Ｄ３ 、…が復号されていく。

【０１３１】暗号化ブロックデータＥＤ254 から、ブロックデータＤ254 が復号されたら、図９に示すように、暗号化ブロックデータＥＤ255 と、鍵情報Ｋとがブロック暗号復号回路１２１に送られ、ブロック暗号復号回路１３１で暗号の復号処理が行われる。

【０１３２】ブロック暗号復号回路１３１の出力がＥＸ－ＯＲゲート１３２に送られる。また、ＥＸ－ＯＲゲート１３２には、ブロックデータＤｊ 以外のデータとの間の関数ｆ（Ｄｉ ）が送られる。

【０１３３】ＥＸ－ＯＲゲート１３２で、ブロック暗号復号回路１３１の出力と、ブロックデータＤｊ 以外のデータとの間の関数ｆ（Ｄｉ ）とのＥＸ－ＯＲがとられて、ブロックデータＤ255 が復号される。

【０１３４】なお、上述の例では、連鎖も初期値も鍵情報も、全て、６４ビットで処理しているが、１２８ビットでも、２５６ビットでも良い。

【０１３５】図１０～図１２は、上述のように、データを暗号化して記録するときの処理を示すフローチャートである。この処理では、例えば２０４８バイトからなる１セクタがＣＢＣにより暗号化される。１セクタは、８

バイト（６４ビット）毎の２５６のブロックに分割される。

【０１３６】図１０において、先ず、１セクタ（例えば２０４８バイト）に相当するブロックデータD0 ～D255のうちの１つのブロックデータDjが読み出される（ステップＳ１）。そして、ブロックデータDiの関数ｆ（Di）とのＥＸ－ＯＲが鍵情報Ｋにより暗号化されて、初期値ｉｎＶが生成される（ステップＳ２）。この初期値ｉｎＶが保存される（ステップＳ３）。

【０１３７】そして、初期値を作るのに用いたブロックデータDjが最初のブロックデータ（ｊ＝０）か否かが判断される（ステップＳ４）。

【０１３８】（ｊ＝０）なら、初期値ｉｎＶが読み出され（ステップＳ５）、この初期値ｉｎＶがブロックデータD0 の暗号化ブロックデータＥD0 とされる（ステップＳ６）。求められた暗号化ブロックデータＥD0 が保存される（ステップＳ７）。

【０１３９】ブロックデータの番号ｉが（ｉ＝１）に初期化される（ステップＳ８）。初期値ｉｎＶが読み出され（暗号化ブロックデータD0 と等しい）（ステップＳ９）、ブロックデータD1 が読み出される（ステップＳ１０）。初期値ｉｎＶとブロックデータD1 とのＥＸ－ＯＲが鍵情報Ｋで暗号化され、ブロックデータD1 の暗号化ブロックデータＥD1 が生成される（ステップＳ１１）。この暗号化ブロックデータＥDi が保存される（ステップＳ１２）。そして、ブロックデータの番号ｉが（ｉ＝２）にインクリメントされる（ステップＳ１３）。

【０１４０】ブロックデータの番号ｉがインクリメントされたら、暗号化ブロックデータＥDi-1 が読み出され（ステップＳ１４）、ブロックデータDi が読み出される（ステップＳ１５）。暗号化ブロックデータＥDi-1 とブロックデータDi とのＥＸ－ＯＲが鍵情報Ｋで暗号化され、ブロックデータDi の暗号化ブロックデータＥDi が生成される（ステップＳ１６）。この暗号化ブロックデータＥDi が保存される（ステップＳ１７）。そして、ブロックデータの番号ｉがインクリメントされる（ステップＳ１８）。

【０１４１】ブロック番号ｉが「２５６」に達したか否かが判断され（ステップＳ１９）、ブロック番号ｉが「２５６」に達していなければ、ステップＳ１４にリターンされる。そして、ブロック番号ｉが「２５６」に達するまで、同様の処理が繰り返され、暗号化ブロックデータＥDi が求められていき、ブロック番号ｉが「２５６」に達してブロックデータD255 まで求められたら処理が終了される。

【０１４２】ステップＳ４で、初期値を作るのに用いたブロックデータDjが最初のブロックデータ（ｊ＝０）でなければ、図１１に示すように、初期値を作るのに用いたブロックデータDjが最後のブロックデータ（ｊ＝２５５）か否かが判断される（ステップＳ２０）。

【０１４３】（ｊ＝２５５）なら、ブロック番号ｉが（ｉ＝０）に初期化される（ステップＳ２１）。そして、ステップＳ２で求められた初期値ｉｎＶが読み出され（ステップＳ２２）、ブロックデータD0 が読み出される（ステップＳ２３）。初期値ｉｎＶとブロックデータD0 とのＥＸ－ＯＲが鍵情報Ｋで暗号化され、ブロックデータD0 の暗号化ブロックデータＥD0 が生成される（ステップＳ２４）。この暗号化ブロックデータＥD0 が保存される（ステップＳ２５）。そして、ブロックデータの番号ｉが（ｉ＝１）にインクリメントされる（ステップＳ２６）。

【０１４４】ブロックデータの番号ｉがインクリメントされたら、暗号化ブロックデータＥDi-1 が読み出され（ステップＳ２７）、ブロックデータDi が読み出される（ステップＳ２８）。暗号化ブロックデータＥDi-1 とブロックデータDi とのＥＸ－ＯＲが鍵情報Ｋで暗号化され、ブロックデータDi の暗号化ブロックデータＥDi が生成される（ステップＳ２９）。この暗号化ブロックデータＥDi が保存される（ステップＳ３０）。そして、ブロックデータの番号ｉがインクリメントされる（ステップＳ３１）。

【０１４５】ブロック番号ｉが「２５５」に達したか否かが判断され（ステップＳ３２）、ブロック番号ｉが「２５５」に達していなければ、ステップＳ２７にリターンされる。そして、ブロック番号ｉが「２５５」に達するまで、同様の処理が繰り返され、暗号化ブロックデータＥDi が求められていく。

【０１４６】ブロック番号が「２５５」になったら、ステップＳ２で求められた初期値ｉｎＶが読み出される（ステップＳ３３）。そして、この初期値ｉｎＶが暗号化ブロックデータＥD255 とされて（ステップＳ３４）、保存され（ステップＳ３５）、処理が終了される。

【０１４７】ステップＳ４で初期値を作るのに用いたブロックデータDjが最初のブロックデータ（ｊ＝０）ではないと判断され、ステップＳ２０で、最後のブロックデータ（ｊ＝２５５）でもないと判断されたら、図１２に示すように、ブロックデータの番号ｉが（ｉ＝０）に初期化される（ステップＳ３６）。ステップＳ２で求められた初期値ｉｎＶが読み出され（ステップＳ３７）、ブロックデータD0 が読み出される（ステップＳ３８）。初期値ｉｎＶとブロックデータD0 とのＥＸ－ＯＲが鍵情報Ｋで暗号化され、ブロックデータD0 の暗号化ブロックデータＥD0 が生成される（ステップＳ３９）。この暗号化ブロックデータＥD0 が保存される（ステップＳ４０）。そして、ブロックデータの番号ｉが（ｉ＝１）にインクリメントされる（ステップＳ４１）。

【０１４８】ブロックデータの番号ｉがインクリメント

されたら、今回のブロック番号ｉは初期値を作るのに用いる所の番号ｊ（ｊ＝ｉ）であるか否かが判断される（ステップＳ４２）。（ｊ＝ｉ）でなければ、暗号化ブロックデータＥＤｉ-1 が読み出され（ステップＳ４３）、ブロックデータＤｉが読み出される（ステップＳ４４）。暗号化ブロックデータＥＤｉ-1 とブロックデータＤｉとのＥＸ－ＯＲが鍵情報Ｋで暗号化され、ブロックデータＤｉの暗号化ブロックデータＥＤｉが生成される（ステップＳ４５）。この暗号化ブロックデータＥＤｉが保存される（ステップＳ４６）。そして、ブロックデータの番号ｉがインクリメントされる（ステップＳ４７）。

【０１４９】ブロック番号ｉが「２５６」に達したか否かが判断され（ステップＳ４８）、ブロック番号ｉが「２５６」に達していなければ、ステップＳ４２にリターンされる。

【０１５０】ステップＳ４２で、（ｊ＝ｉ）であると判断されたら、ステップＳ２で求められた初期値ｉｎＶが読み出され（ステップＳ４９）、この初期値ｉｎＶがブロックデータＤｊの暗号化ブロックデータＥＤｊとされる（ステップＳ５０）。この暗号化ブロックデータＥＤｊが保存される（ステップＳ５１）。そして、ステップＳ４７に進む。

【０１５１】そして、ブロック番号ｉが「２５６」に達するまで、同様の処理が繰り返される。ブロック番号ｉが「２５６」に達し、ブロックデータＤ255 までの暗号化ブロックデータが求められたら、処理が終了される。

【０１５２】次に、暗号を復号するときの処理について説明する。図１３～図１６は、暗号を復号する場合の処理を示すフローチャートである。

【０１５３】図１３～図１６において、初期値として用いたブロック番号ｊが（ｊ＝０）か否かが判断される（ステップＳ１０１）。

【０１５４】（ｊ＝０）のときには、暗号化ブロックデータＥＤ０が読み出される（ステップＳ１０２）。この暗号化ブロックデータＥＤ０が鍵情報Ｋで復号され、この復号値と関数ｆ（Ｄｉ）とのＥＸ－ＯＲにより、ブロックデータＤ０が生成される（ステップＳ１０３）。このブロックデータＤ０が保存される（ステップＳ１０４）。

【０１５５】ブロック番号ｉが（ｉ＝１）に初期化される（ステップＳ１０５）。暗号化ブロックデータＥＤ１が読み出される（ステップＳ１０６）。そして、暗号化ブロックデータＥＤ０が読み出される（ステップＳ１０７）。暗号化ブロックデータＥＤ０が初期値ｉｎＶとされる（ステップＳ１０８）。

【０１５６】暗号化ブロックデータＥＤ１が鍵情報Ｋで復号され、この復号値と初期値ｉｎＶ（暗号化ブロックデータＥＤ０と等しい）とのＥＸ－ＯＲがとられて、ブロックデータＤ１が生成される（ステップＳ１０９）。生成されたブロックデータＤ１が保存される（ステップＳ１１０）。そして、ブロック番号ｉが（ｉ＝２）にインクリメントされる（ステップＳ１１１）。

【０１５７】暗号化ブロックデータＥＤｉが読み出される（ステップＳ１１２）。暗号化ブロックデータＥＤｉ-1 が読み出される（ステップＳ１１３）。暗号化ブロックデータＥＤｉが鍵情報Ｋで復号され、この復号値と暗号化ブロックデータＥＤｉ-1とのＥＸ－ＯＲがとられて、ブロックデータＤｉが生成される（ステップＳ１１４）。このブロックデータＤｉが保存される（ステップＳ１１５）。そして、ブロック番号ｉがインクリメントされる（ステップＳ１１６）。

【０１５８】ブロック番号ｉが「２５６」に達したか否かが判断され（ステップＳ１１７）、ブロック番号ｉが「２５６」に達していなければ、ステップＳ１１２にリターンされる。ブロック番号ｉが「２５６」に達するまで、同様の処理が繰り返される。ブロック番号ｉが「２５６」に達し、ブロックデータＤ255 まで復号されたら、処理が終了される。

【０１５９】ステップＳ１０１で、初期値として用いたブロック番号ｊが（ｊ＝０）ではないと判断されたら、図１４に示すように、初期値として用いたブロック番号ｊが（ｊ＝２５５）か否かが判断される（ステップＳ１１８）。

【０１６０】（ｊ＝２５５）なら、ブロック番号ｉが（ｉ＝０）に初期化される（ステップＳ１１９）。暗号化ブロックデータＥＤ０が読み出される（ステップＳ１２０）。暗号化ブロックデータＥＤ255 が読み出される（ステップＳ１２１）。暗号化ブロックデータＥＤ255 が初期値ｉｎＶとされる（ステップＳ１２２）。

【０１６１】暗号化ブロックデータＥＤ０が鍵情報Ｋで復号され、この復号値と初期値ｉｎＶのＥＸ－ＯＲがとられて、ブロックデータＤ０が生成される（ステップＳ１２３）。生成されたブロックデータＤ０が保存される（ステップＳ１２４）。そして、ブロック番号ｉが（ｉ＝１）にインクリメントされる（ステップＳ１２５）。

【０１６２】暗号化ブロックデータＥＤｉが読み出される（ステップＳ１２６）、暗号化ブロックデータＥＤｉ-1 が読み出される（ステップＳ１２７）。暗号化ブロックデータＥＤｉが鍵情報Ｋで復号され、この復号値と暗号化ブロックデータＥＤｉ-1とのＥＸ－ＯＲがとられて、ブロックデータＤｉが生成される（ステップＳ１２８）。このブロックデータＤｉが保存される（ステップＳ１２９）。そして、ブロック番号ｉがインクリメントされる（ステップＳ１３０）。

【０１６３】ブロック番号ｉが「２５５」に達したか否かが判断され（ステップＳ１３１）、ブロック番号ｉが「２５５」に達していなければ、ステップＳ１２６にリターンされる。ブロック番号ｉが「２５５」に達するま

で、同様の処理が繰り返される。

【０１６４】ブロック番号ｉが「２５５」に達し、ブロックデータD254 までの処理が完了したら、暗号化ブロックデータＥＤ255 が読み出される（ステップＳ１３２）。この暗号化ブロックデータＥＤ255 が鍵情報Ｋで復号され、この復号値と関数ｆ（Ｄｉ）とのＥＸ－ＯＲにより、ブロックデータD255 が生成される（ステップＳ１３３）。このブロックデータD255 が保存されて（ステップＳ１３４）、処理が終了される。

【０１６５】ステップＳ１０１で、（ｊ＝０）ではないと判断され、ステップＳ１１８で、（ｊ＝２５５）ではないと判断されたら、図１５に示すように、ブロック番号ｉが（ｉ＝０）に初期化される（ステップＳ１３５）。

【０１６６】暗号化ブロックデータＥＤ0 が読み出される（ステップＳ１３６）。暗号化ブロックデータＥＤｊが読み出される（ステップＳ１３７）。暗号化ブロックデータＥＤｊが初期値ｉｎＶとされる（ステップＳ１３８）。

【０１６７】暗号化ブロックデータＥＤ0 が鍵情報Ｋで復号され、この復号値と初期値ｉｎＶとのＥＸ－ＯＲがとられて、ブロックデータD0 が生成される（ステップＳ１３９）。生成されたブロックデータD0 が保存される（ステップＳ１４０）。そして、図１６に示すように、ブロック番号ｉが（ｉ＝１）にインクリメントされる（ステップＳ１４１）。

【０１６８】ブロックデータの番号ｉがインクリメントされたら、今回のブロック番号ｉは初期値を作るのに用いる所の番号ｊ（ｊ＝ｉ）であるか否かが判断される（ステップＳ１４２）。

【０１６９】（ｊ＝ｉ）でなければ、暗号化ブロックデータＥＤｉが読み出される（ステップＳ１４３）。暗号化ブロックデータＥＤｉ-1 が読み出される（ステップＳ１４４）。暗号化ブロックデータＥＤｉ が鍵情報Ｋで復号され、この復号値と暗号化ブロックデータＥＤｉ-1 とのＥＸ－ＯＲがとられて、ブロックデータＤｉ が生成される（ステップＳ１４５）。このブロックデータＤｉ が保存される（ステップＳ１４６）。そして、ブロック番号ｉがインクリメントされる（ステップＳ１４７）。

【０１７０】ブロック番号ｉが「２５６」に達したか否かが判断され（ステップＳ１４８）、ブロック番号ｉが「２５６」に達していなければ、ステップＳ１４２にリターンされる。

【０１７１】ステップＳ１４２で、（ｉ＝ｊ）であると判断されたら、暗号化ブロックデータＥＤｊ が読み出される（ステップＳ１４９）。この暗号化ブロックデータＥＤｊが鍵情報Ｋで復号され、この復号値と関数ｆ（Ｄｉ）とのＥＸ－ＯＲにより、ブロックデータＤｊ が生成される（ステップＳ１５０）。このブロックデータＤｊ が保存される（ステップＳ１５１）。そして、ステップＳ１４７に進められる。

【０１７２】そして、ブロック番号ｉが「２５６」に達するまで、同様の処理が繰り返される。ブロック番号ｉが「２５６」に達し、ブロックデータD255 までの復号が完了したら、処理が終了される。

【０１７３】なお、初期値を暗号化したブロックデータＤｊについては、常に固定の所にしておいても良いし、変更できるようにしても良い。初期値を暗号化したブロックデータＤｊを変更可能としておくことで、秘匿性を上げることができる。

【０１７４】以上のように、この発明では、ブロック暗号化を連鎖的に行う場合の初期値を、コンテンツデータそのものから生成している。このため、データ領域のロスがないと共に、コンテンツデータはランダムに変化しているため、秘匿性が高い。

【０１７５】つまり、コンテンツデータが音楽データのような場合には、サンプリングにより得られたデータであるため、それ自身、ランダマイズ化されたデータであると言える。ある時点の音楽データの値がどのレベルであるかを知ることは、非常に困難なことである。したがって、コンテンツデータ自身から初期値を作ると、乱数を初期値として用いたと同じように、秘匿性が向上する。

【０１７６】次に、コンテンツのデータとして、ＭＰＥＧストリームを記録する場合について説明する。

【０１７７】図１に示したように、ＣＤ２の光ディスクは、内周側の領域ＡＲ１と、外周側の領域ＡＲ２とがあり、領域ＡＲ２には、ＭＰ３方式でファイル化されたオーディオデータが記録される。ＭＰ３方式は、ＭＰＥＧ１で使用されるオーディオデータの３つのレイヤのうちの一つである。したがって、外周側の領域ＡＲ２にＭＰ３のデータを記録する場合には、ＭＰＥＧストリームに準拠して、データの記録が行われる。

【０１７８】ＭＰＥＧのストリームは、上位レイヤ（プログラムレイヤ、パックレイヤ）と、下位レイヤ（パケットレイヤ）でストリームが構成される。すなわち、ＭＰＥＧストリームでは、１つのプログラムのシーケンスは複数のパックからなり、各パックは、一般的には、複数のパケットから構成される。各パックの先頭には、パックヘッダが設けられる。パケットは、パケットヘッダとデータとからなる。

【０１７９】ＣＤでは、９８フレームからなるブロックがセクタとされ、このセクタを単位として、データが記録される。

【０１８０】図１７は、ＣＤにＭＰＥＧストリームを記録したときのデータ構造を示すものである。図１７に示すように、ＣＤの１セクタには、２０４８バイトのデータ領域が設けられる。この２０４８バイトのデータ領域に、原則として、１セクタに、ＭＰＥＧストリームのパック及びパケットが配置される。図１８に示すように、

ファイルの先頭には、ファイルヘッダが設けられる。このファイルヘッダには、著作者の管理情報が配置される。

【０１８１】図１７に示すように、１セクタの先頭には、パックヘッダが設けられる。このパックヘッダは、例えば１４バイトからなる。このパックヘッダには、パックスタートコードや、ＳＣＲ（System Clock Reference）、ビットレートが含まれている。

【０１８２】パックヘッダに続いて、パケットヘッダが設けられる。このパケットヘッダは、例えば、１８バイトからなる。このパケットヘッダには、パケットスタートコード、ストリームＩＤ、ＰＥＳ（Packetized Elementary Stream）ヘッダ長、ＰＴＳ（Presentation Time Stamp）が含まれている。

【０１８３】１セクタの残りの２０１６バイトに、ＭＰＥＧ方式で圧縮されたコンテンツのデータ（例えば、圧縮されたオーディオデータ）が配置される。

【０１８４】このように、ＭＰ３のようなＭＰＥＧのファイルは、パックとパケットからなる構成のストリームに組み込まれる。そして、図１８に示すように、ファイルの先頭には、ファイルヘッダが設けられる。このファイルヘッダには、ファイルＩＤやＩＳＲＣ（International Standard Recoding Code）のような著作者の管理情報が含められる。ＩＳＲＣは、その曲のマスターテープや作成時に付けられる曲、会社、録音年、レコーディング番号等からなる１２桁のコードである。さらに、ディスクを自体を識別できるようなディスクＩＤを設けるようにしても良い。

【０１８５】このように、ＣＤにＭＰＥＧのストリームを記録する場合には、２０４８バイトの１セクタのデータ領域に、原則として、パック及びセクタのデータが記録される。これら１セクタのデータのうち暗号化が必要なのは２０１６バイトのデータであり、１４バイトのパックヘッダ及び１８バイトのパケットヘッダは暗号化は不要である。

【０１８６】図１９は、１セクタ分のＭＰＥＧストリームのコンテンツのデータを暗号化する場合のブロックの構成を示すものである。上述のように、ＭＰＥＧストリームの場合には、１セクタのデータのうち、暗号化する必要があるのは、２０１６バイトのデータである。したがって、ＭＰＥＧストリームを暗号化する場合には、図１９に示すように、１セクタのデータは、８バイト（６４ビット）単位で、２５２のブロックに分割される。そして、前述と同様に、今回のブロックデータと、その１つ前のブロックデータを暗号化したデータとのＥＸ－ＯＲをとって、暗号化するようなＣＢＣ方式により、暗号化される。

【０１８７】ＣＢＣ方式で暗号化する場合には、初期値が必要である。前述の例では、初期値を、同一セクタ内のブロックのコンテンツデータから生成するようにしている。ＭＰＥＧストリームの場合にも、これと同様に、同一セクタ内のブロックのコンテンツデータそのものから初期値を作っても良いが、ＭＰＥＧストリームのヘッダのユニーク性を着目して、ＭＰＥＧストリームのヘッダからＣＢＣの初期値を作るようにしても良い。

【０１８８】つまり、図１７に示したように、ＭＰＥＧストリームには、パックヘッダと、パケットヘッダとが設けられている。また、図１８に示すように、ファイルの先頭には、ファイルヘッダが設けられる。これらのヘッダから初期値を生成することが考えられる。

【０１８９】例えば、ファイルヘッダには、ＩＳＲＣのような著作権の管理情報等が記録されている。この著作権の管理情報は、コンテンツ毎にユニークな値である。また、ディスクヘッダがある場合のは、ディスクのシリアル番号のように、ディスク毎にユニークな値をディスクヘッダに入れることができる。このような情報は、ディスク毎にユニークな情報である。

【０１９０】また、パックヘッダは、パックスタートコードや、ＳＣＲ、ビットレートが含まれている。この中で、ＳＣＲは、システムの基準となるＳＴＣ（System TimeClock）を較正するための時間情報である。また、パケットヘッダには、パケットスタートコード、ストリームＩＤ、ＰＥＳヘッダ長、ＰＴＳが含まれている。この中で、ＰＴＳは再生の基準となる時間情報である。パックヘッダのＳＣＲや、パケットヘッダの中のＰＴＳは、時間と共に変化するため、ユニークな値となる。

【０１９１】このような、ＭＰＥＧストリームのヘッダに含まれているユニークな情報を使って、ＣＢＣ方式で暗号化する場合の初期値を生成することができる。

【０１９２】ＭＰＥＧストリームのヘッダの中でユニークな情報を使って、ＣＢＣ方式の初期を生成する場合に、ヘッダの情報をそのまま用いても良いが、ヘッダの情報をそのまま用いると、秘匿性が十分でない。

【０１９３】そこで、いくつかのＭＰＥＧストリームのヘッダの情報から初期値を生成したり、ヘッダの情報を暗号化して、初期値を生成することが考えられる。具体的には、以下の方法が考えられる。

【０１９４】まず、著作権情報のようなファイルヘッダのユニークな情報と、パックヘッダのＳＣＲやパケットヘッダの中のＰＴＳのような時間と共に変化する情報とを所定の関数により組み合わせて初期値を生成することが考えられる。

【０１９５】図２０は、このように、著作権情報のようなファイルヘッダのユニークな情報と、パックヘッダのＳＣＲやハケットヘッダの中のＰＴＳのような時間と共に変化する情報とから初期値を生成する場合のプロセスの一例である。図２０において、ＥＸ－ＯＲゲート２０１には、ファイルヘッダのユニークな情報が供給されると共に、パックヘッダのＳＣＲ又はパケットヘッダの中のＰＴＳが供給される。ＥＸ－ＯＲゲート２０１で、フ

ファイルヘッダのユニークな情報と、パックヘッダのＳＣＲ又はパケットヘッダの中のＰＴＳとのＥＸ－ＯＲが求められる。このＥＸ－ＯＲゲート２０１の出力から、初期値ｉｎＶが求められる。

【０１９６】次に、著作権情報のようなファイルヘッダのユニークな情報、又は、パックヘッダのＳＣＲやパケットヘッダの中のＰＴＳのような時間と共に変化する情報を暗号化して、初期値を生成することが考えられる。

【０１９７】図２１Ａは、著作権情報のようなファイルヘッダのユニークな情報を暗号化して初期値を生成する場合のプロセスの一例である。図２１Ａにおいて、暗号化回路２１１には、ファイルヘッダのユニークな情報が供給される。暗号化回路２１１で、このファイルヘッダのユニークな情報が暗号化され、暗号化回路２１１の出力から、初期値ｉｎＶが求められる。

【０１９８】図２１Ｂは、パックヘッダのＳＣＲやパケットヘッダの中のＰＴＳのような時間と共に変化する情報を暗号化して初期値を生成する場合のプロセスの一例である。図２１Ｂにおいて、暗号化回路２２１には、パックヘッダのＳＣＲ又はパケットヘッダの中のＰＴＳが供給される。暗号化回路２２１で、ＳＣＲ又はＰＴＳが暗号化され、暗号化回路２２１の出力から、初期値ｉｎＶが求められる。

【０１９９】さらに、著作権情報のようなファイルヘッダのユニークな情報と、パックヘッダのＳＣＲやパケットヘッダの中のＰＴＳのような時間と共に変化する情報とから求められる情報を暗号化して、初期値を生成することが考えられる。

【０２００】図２２は、著作権情報のようなファイルヘッダのユニークな情報と、パックヘッダのＳＣＲやパケットヘッダの中のＰＴＳのような時間と共に変化する情報を、更に、暗号化して、初期値を生成する場合のプロセスの一例である。図２２において、ＥＸ－ＯＲゲート２３１には、ファイルヘッダのユニークな情報が供給されると共に、パックヘッダのＳＣＲ又はパケットヘッダの中のＰＴＳが供給される。ＥＸ－ＯＲゲート２３１で、ファイルヘッダのユニークな情報と、パックヘッダのＳＣＲ又はパケットヘッダの中のＰＴＳとのＥＸ－ＯＲが求められる。このＥＸ－ＯＲゲート２３１の出力が暗号化回路２３２に供給される。暗号化回路２３２で、ＥＸ－ＯＲゲート２３１の出力が暗号化され、暗号化回路２３２の出力から、初期値ｉｎＶが求められる。

【０２０１】図２３は、ＭＰＥＧストリームを暗号化する場合の暗号化プロセスの一例である。図２３において、ＥＸ－ＯＲゲート３０１－０で、入力ブロックデータＤ０と、ＭＰＥＧヘッダから求められた初期値ｉｎＶとのＥＸ－ＯＲがとられ、このＥＸ－ＯＲゲート３０１－０の出力がブロック暗号化回路３０２－０に供給される。

【０２０２】ブロック暗号化回路３０２－０で、ＥＸ－ＯＲゲート３１１の出力と鍵情報Ｋとから、暗号化ブロックデータＥＤ０が求められる。

【０２０３】次に、ＥＸ－ＯＲゲート３０１－１で、入力ブロックデータＤ１と、暗号化ブロックデータＥＤ０とのＥＸ－ＯＲがとられ、このＥＸ－ＯＲゲート３０１－１の出力がブロック暗号化回路３０２－１に供給され、ブロック暗号化回路３０２－１で、ＥＸ－ＯＲゲート３０１－１の出力と鍵情報Ｋとから、暗号化ブロックデータＥＤ１が求められる。

【０２０４】以下、同様にして、入力データＤ２、Ｄ３、…、Ｄ２５１から、暗号化ブロックデータＥＤ２、ＥＤ３、…、ＥＤ２５１が求められる。

【０２０５】図２４は、ＭＰＥＧストリームを復号する場合の復号化プロセスの一例である。図２４において、暗号化ブロックデータＥＤ０と、鍵情報Ｋとがブロック暗号復号回路４０１－０に送られ、ブロック暗号復号回路４０１－０で、暗号の復号処理が行われる。

【０２０６】ブロック暗号復号回路４０１－０の出力がＥＸ－ＯＲゲート４０２－０に送られる。また、ＥＸ－ＯＲゲート４０２－０には、初期値ｉｎＶが送られる。この初期値ｉｎＶは、暗号化ブロックデータｉｎＶである。

【０２０７】ＥＸ－ＯＲゲート４０２－０で、ブロック暗号復号回路４０１－０の出力と、初期値ｉｎＶとのＥＸ－ＯＲがとられ、ブロックデータＤ０が復号される。

【０２０８】次に、暗号化ブロックデータＥＤ１と、鍵情報Ｋとがブロック暗号復号回路４０１－１に送られる。ブロック暗号復号回路４０１－１で暗号が復号される。ブロック暗号復号回路４０１－１の出力がＥＸ－ＯＲゲート４０２－１に送られる。

【０２０９】また、ＥＸ－ＯＲゲート４０２－１には、その前の暗号化ブロックデータＥＤ０とが送られる。

【０２１０】ＥＸ－ＯＲゲート４０２－１で、ブロック暗号復号回路４０１－１の出力と、その前の暗号化ブロックデータＥＤ０とのＥＸ－ＯＲがとられて、ブロックデータＤ１が復号される。

【０２１１】以下、同様にして、暗号化ブロックデータＥＤ１、ＥＤ２、…から、ブロックデータＤ１、Ｄ２、…、Ｄ２５１が復号されていく。

【０２１２】このように、ＭＰＥＧストリームを記録する場合には、ＭＰＥＧのヘッダのユニーク性を利用して、ＭＰＥＧヘッダを使ってＣＢＣ方式で暗号化を行う場合の初期値を作ることができる。なお、上述の例では、ファイルヘッダと、パックヘッダ又はパケットヘッダのＳＣＲ又はＰＴＳ等の時間情報とを使って初期値を生成しているが、さらに、ディスクヘッダの情報を用いるようにしても良い。

【０２１３】なお、上述の例では、コンテンツのデータをＣＤ２の光ディスクに記録しているが、記録媒体とし

ては、ＣＤ２の光ディスクに限定されるものではない。この発明は、ＣＤ－ＤＡやＣＤ－ＲＯＭ、ＣＤ－ＲやＣＤ－ＲＷにコンテンツのデータを記録する場合にも、同様に適用することができる。また、光ディスクに限らず、磁気ディスク、フラッシュメモリカード等、種々の記録媒体にコンテンツのデータを記録する場合に同様に適用できる。

【０２１４】さらに、この発明は、コンテンツのデータをネットワークで配信する場合に用いても好適である。

【０２１５】つまり、近年、音楽データのようなコンテンツのデータをネットワークを使って配信するようなサービスが普及している。このようなサービスでは、コンテンツのデータの保護を図るために、コンテンツのデータを暗号化することが望まれる。この発明では、ブロック暗号化を連鎖的に行う場合の初期値を、コンテンツデータそのもの又はＭＰＥＧストリームのデータから生成しているため、コンテンツのデータを配信する場合の暗号化にも好都合である。

【０２１６】

【発明の効果】この発明によれば、コンテンツのデータがブロック化され、鎖状に連鎖して暗号化される。そして、このときの初期値を、そのセクタのコンテンツデータそのものから生成している。このため、初期値を乱数等で発生する必要がなく、データ領域のロスがない。また、コンテンツデータはランダムに変化しているため、秘匿性が高い。更に、乱数発生器等を容易する必要がなく、回路規模が増大しない。

【０２１７】また、この発明によれば、コンテンツデータから生成される初期値自体が他のコンテンツデータで暗号化される。更に、初期値として使うコンテンツデータを自由に選ぶことができる。これにより、秘匿性が向上される。

【０２１８】さらに、この発明によれば、ＭＰＥＧストリームを記録する場合には、ヘッダに含まれるユニークな情報を使って、初期値を生成している。ヘッダの情報はユニークであり、ＳＣＲやＰＴＳのような時間情報は、時間と共に変化するため、秘匿性が高い。また、ＭＰＥＧストリームのヘッダの情報を使って暗号化の初期値を形成しているので、ＭＰＥＧストリームを保ったまま、伝送することができる。さらに、乱数発生器等を容易する必要がなく、回路規模が増大しない。

【図面の簡単な説明】

【図１】この発明が適用された光ディスクの一例の略線図である。

【図２】この発明が適用された記録装置の一例のブロック図である。

【図３】この発明が適用された再生装置の一例のブロック図である。

【図４】セクタの構成を示す略線図である。

【図５】ブロックの構成を示す略線図である。

【図６】この発明が適用された暗号化処理の説明に用いるブロック図である。

【図７】この発明が適用された暗号化処理の説明に用いるブロック図である。

【図８】この発明が適用された復号化処理の説明に用いるブロック図である。

【図９】この発明が適用された復号化処理の説明に用いるブロック図である。

【図１０】この発明が適用された暗号化処理の説明に用いるフローチャートである。

【図１１】この発明が適用された暗号化処理の説明に用いるフローチャートである。

【図１２】この発明が適用された暗号化処理の説明に用いるフローチャートである。

【図１３】この発明が適用された暗号化処理の説明に用いるフローチャートである。

【図１４】この発明が適用された復号化処理の説明に用いるフローチャートである。

【図１５】この発明が適用された復号化処理の説明に用いるフローチャートである。

【図１６】この発明が適用された復号化処理の説明に用いるフローチャートである。

【図１７】ＭＰＥＧストリームを記録する場合の説明に用いる略線図である。

【図１８】ＭＰＥＧストリームを記録する場合の説明に用いる略線図である。

【図１９】ＭＰＥＧストリームを記録する場合のブロックの構成を示す略線図である。

【図２０】この発明が適用された暗号化処理の説明に用いるブロック図である。

【図２１】この発明が適用された暗号化処理の説明に用いるブロック図である。

【図２２】この発明が適用された暗号化処理の説明に用いるブロック図である。

【図２３】この発明が適用された暗号化処理の説明に用いるブロック図である。

【図２４】この発明が適用された復号化処理の説明に用いるブロック図である。

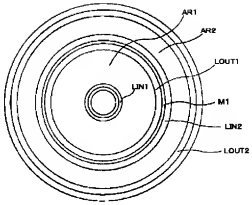
【図２５】従来の暗号化処理の説明に用いるブロック図である。

【図２６】従来の暗号化処理の説明に用いるブロック図である。

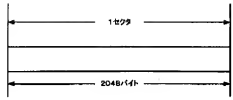
【符号の説明】

４・・・暗号化回路，２６・・・暗号解読回路，１０，２０・・・光ディスク

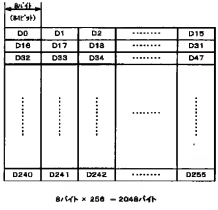
【図１】



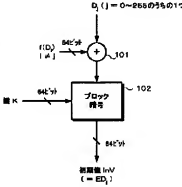
【図４】



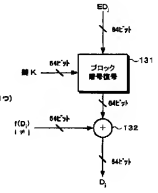
【図５】



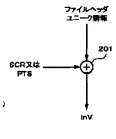
【図６】



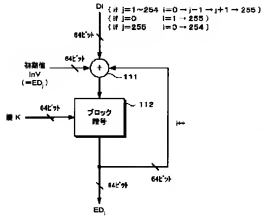
【図９】



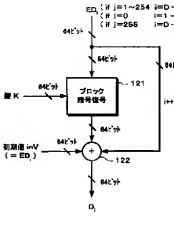
【図２０】



【図７】

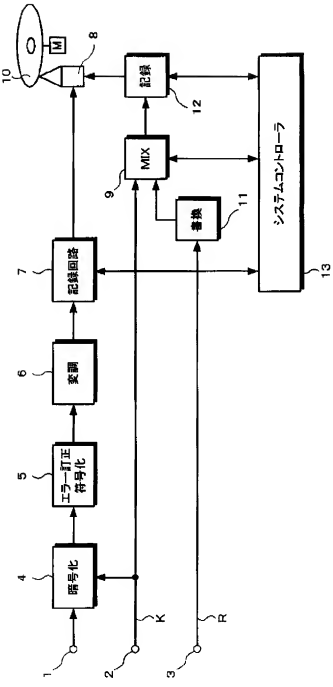


【図８】

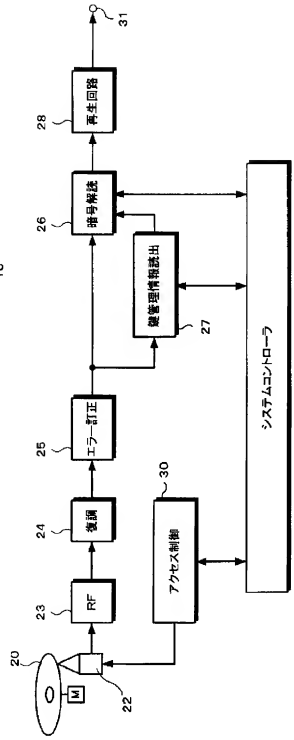


【図１８】

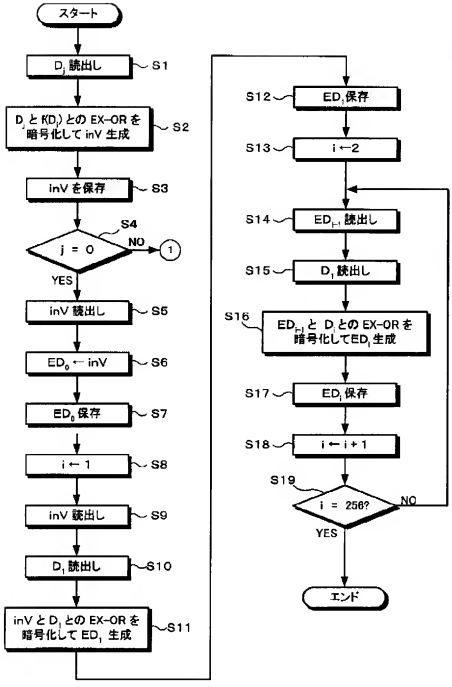
【図２】


1
2
3
4
5
6
7
8
9
10
11
12
13
K
R
M
符号化
エラー訂正
変調
記録回路
記録
MIX
書換
システムコントローラ

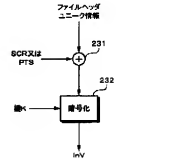
【図３】


20
22
23
24
25
26
27
28
30
31
M
RF
復調
エラー訂正
復号解読
再生回路
アクセス制御
鍵管理情報読出
システムコントローラ

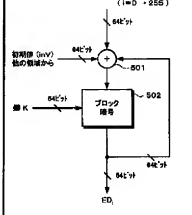
【図１０】



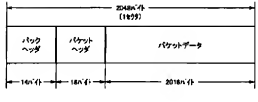
【図２２】



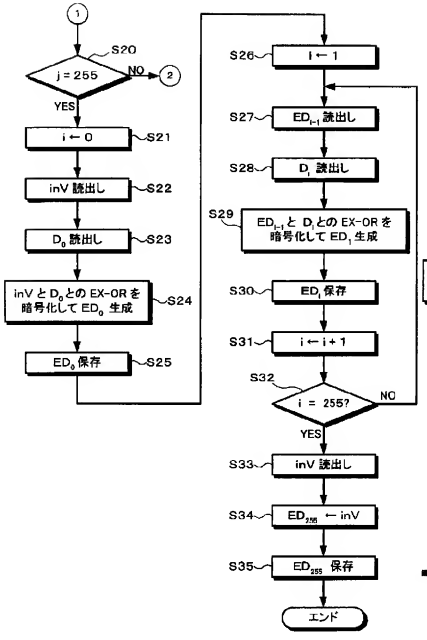
【図２５】



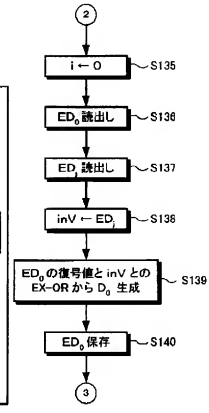
【図１７】



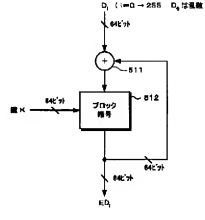
【図１１】



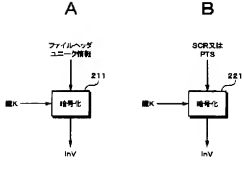
【図１５】



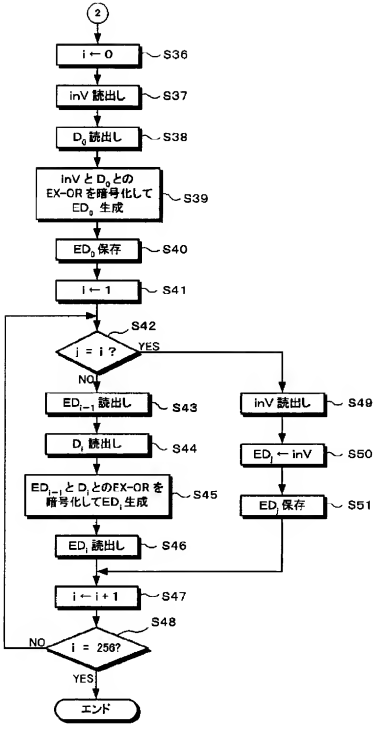
【図２６】



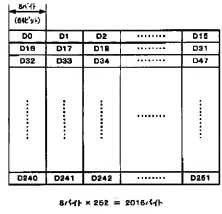
【図２１】



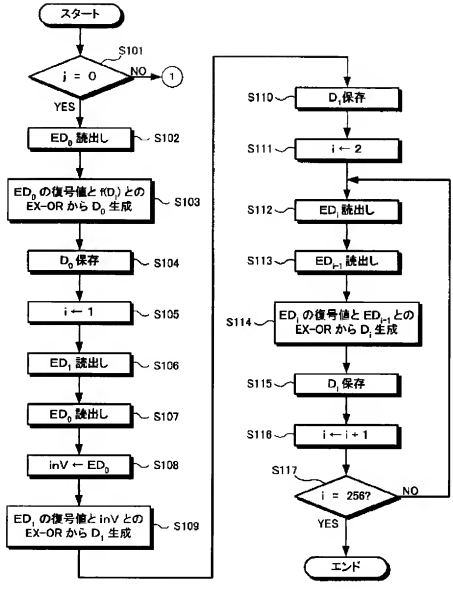
【図１２】


2
i ← 0
S36
inV 読出し
S37
D0 読出し
S38
inV と D0 との EX-OR を暗号化して ED0 生成
S39
ED0 保存
S40
i ← 1
S41
S42
j = i ?
YES
NO
EDi−1 読出し
S43
Di 読出し
S44
EDi−1 と Di とのEX-OR を暗号化してEDi 生成
S45
EDi 読出し
S46
inV 読出し
S49
EDj ← inV
S50
EDj 保存
S51
i ← i + 1
S47
S48
i = 256?
NO
YES
エンド

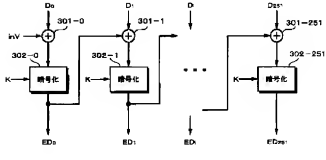
【図１９】


8バイト
(64ビット)
D0 D1 D2 ····· D15
D16 D17 D18 ····· D31
D32 D33 D34 ····· D47
D240 D241 D242 ····· D251
8バイト × 252 = 2016バイト

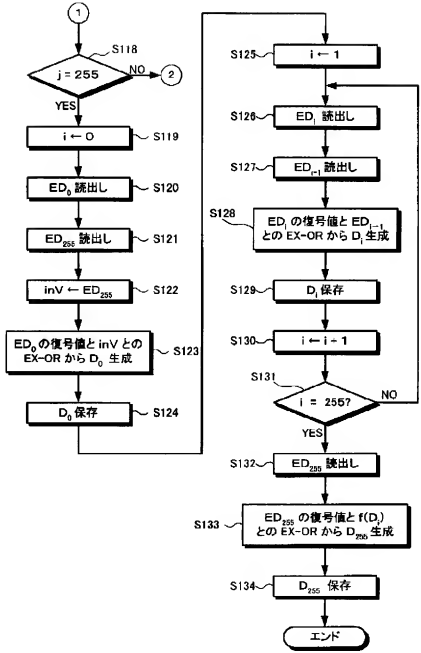
【図１３】


スタート
S101
i = 0
NO
1
YES
ED0 読出し
S102
ED0 の復号値と f(D0) との EX-OR から D0 生成
S103
D0 保存
S104
i ← 1
S105
ED1 読出し
S106
ED0 読出し
S107
inV ← ED0
S108
ED1 の復号値と inV との EX-OR から D1 生成
S109
D1保存
S110
i ← 2
S111
EDi 読出し
S112
EDi-1 読出し
S113
EDi の復号値と EDi-1 との EX-OR から Di 生成
S114
Di 保存
S115
i ← i + 1
S116
i = 256?
S117
NO
YES
エンド

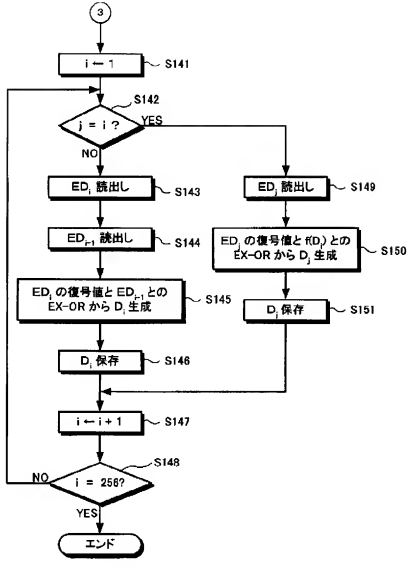
【図２３】


D0
D1
D
D255
301−0
301−1
301−255
inV
302−0
302−1
302−255
K
暗号化
ED0
ED1
EDi
ED255

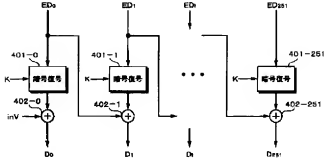
【図１４】


1
S118
j = 255
NO
2
YES
i ← 0
S119
ED0 読出し
S120
ED255 読出し
S121
inV ← ED255
S122
ED0の復号値とinVとの EX-OR から D0 生成
S123
D0 保存
S124
S125
i ← 1
S126
EDi 読出し
S127
EDi-1 読出し
S128
EDi の復号値と EDi-1 との EX-OR から Di 生成
S129
Di 保存
S130
i ← i - 1
S131
i = 255?
NO
YES
S132
ED255 読出し
S133
ED255 の復号値と f(Di) との EX-OR から D255 生成
S134
D255 保存
エンド

【図１６】


3
i ← 1
S141
S142
j = i ?
YES
NO
ED$_i$ 読出し
S143
ED$_{i-1}$ 読出し
S144
ED$_i$ の復号値と ED$_{i-1}$ との EX-OR から D$_i$ 生成
S145
D$_i$ 保存
S146
i ← i + 1
S147
S148
i = 256?
NO
YES
エンド
ED$_j$ 読出し
S149
ED$_j$ の復号値と f(D$_j$) との EX-OR から D$_j$ 生成
S150
D$_j$ 保存
S151

【図２４】


ED$_0$
ED$_1$
ED$_i$
ED$_{251}$
401−0
401−1
401−251
K
暗号復号
402−0
402−1
402−251
inV
D$_0$
D$_1$
D$_i$
D$_{251}$

フロントページの続き

(72)発明者　猪口　達也
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　木原　隆
東京都品川区北品川６丁目７番35号　ソニー株式会社内

Ｆターム(参考)　5B017 AA03 AA06 AA07 BA07 CA09
CA16
5J104 JA13 NA02